PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-281464

(43)Date of publication of application : 27.09.2002

---

(51)Int.Cl. H04N 7/08
H04L 9/16
H04N 7/081
H04N 7/083
H04N 7/087
H04N 7/088

---

(21)Application number : 2001-383577 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 17.12.2001 (72)Inventor : MATSUZAKI NATSUME
TATEBAYASHI MAKOTO
NISHIO TOSHIAKI
SUZUKI HIDEKAZU

---

(30)Priority
Priority number : 2000383345
Priority date : 18.12.2000
Priority country : JP

---

(54) SYSTEM FOR TRANSMITTING CRYPTOGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a transmission system capable of transmitting video information and sound information with high quality.
SOLUTION: This transmission system for transmitting video information and sound information with high quality performs time division multiplexing of a video signal and a sound signal and transmits the resultant signals as a cryptogram. A transmitting side compresses the sound signal on time base, multiplexes the compressed sound signal on the time base to the blanking period of the video signal and transmits the video signal as a cryptogram. Control is performed by using a sound signal data enable signal ADE, and a switching signal of the sound signal and the video signal.

LEGAL STATUS [Date of request for examination] 12.10.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3965047
[Date of registration] 01.06.2007
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] It is transmission SHITESUMU which it is the transmission system which consists of a sending set which keeps a fly-back-line period and transmits digital image information, and a receiving set which receives said digital image information, and said sending set transmits digitized voice information in said fly-back-line period, and is characterized by said receiving set receiving said digitized voice information in said fly-back-line period.

[Claim 2] The sending set which generates the frame information which keeps a fly-back-line period and includes digital image information, enciphers, and is transmitted, Receive said enciphered frame information, decode and said digital image information is extracted from the decoded frame information. It is the code transmission system which consists of graphic display devices to display. Said sending set The frame information which multiplexes digitized voice information to said frame information in said fly-back-line period and by which said digitized voice information was multiplexed is enciphered, and it transmits. Said graphic display device Code transmission SHITESUMU characterized by receiving and decoding said enciphered frame information, extracting said digitized voice information from said fly-back-line period kept into said frame information which generated and generated frame information, and changing into a sound signal.

[Claim 3] The sending set characterized by to have a multiplexing means is the sending set which generates the frame information which keeps one or more fly-back-line periods, and includes digital image information, enciphers, and is transmitted, and multiplex digitized voice information to said frame information in said fly-back-line period, an encryption means encipher said frame information by which said digitized voice information was multiplexed, and a transmitting means transmit said enciphered frame information.

[Claim 4] It is the sending set according to claim 3 which said generated frame information keeps a vertical-retrace-line period, then a horizontal blanking interval is kept for every Rhine, and said digitized voice information consists of two or more Rhine speech information including the Rhine image information, and is characterized by said multiplexing means multiplexing said Rhine speech information in said vertical-retrace-line period and/or said horizontal blanking interval.

[Claim 5] Said encryption means is a sending set according to claim 4 characterized by including a frame key generation means to generate the frame key used as a key of encryption, and the frame cryptographer stage which enciphers the digitized voice information and digital image information which are included in said frame information using said frame key generated corresponding to frame information corresponding to

frame information.
[Claim 6] The Rhine cryptographer stage which enciphers the Rhine speech information and the Rhine image information that said frame cryptographer stage is included in said frame information using said frame key, Until encryption of a renewal means of a key to update said frame key, all the Rhine speech information contained in said frame information, and Rhine image information is completed To said Rhine encryption means, using said updated frame key, control to encipher the following Rhine speech information and the following Rhine image information, and said renewal means of a key is received. The sending set according to claim 5 characterized by including the loop control means controlled to update said updated frame key again.
[Claim 7] Said frame cryptographer stage is a sending set according to claim 5 characterized by using the same cipher system in encryption of said digitized voice information and said digital image information.
[Claim 8] Said Rhine cryptographer stage is a sending set according to claim 7 which sets up the initial value for voice, sets up the initial value for images which enciphers the Rhine speech information, next has the same value as said initial value for voice using said set-up initial value for voice, and is characterized by enciphering the Rhine image information using said set-up initial value for images.
[Claim 9] It is the sending set according to claim 5 which said sending set transmits said enciphered frame information to a graphic display device, and is characterized by using a common operation module for said encryption means in authentication of said graphic display device, generation of said frame key, and encryption of said frame information.
[Claim 10] It is the sending set according to claim 4 which generates the image enable signal which shows transmission of said digital image information, and is characterized by generating the voice enable signal which shows transmission of said digitized voice information, and said transmitting means transmitting said image enable signal generated further and said voice enable signal in said fly-back-line period in the period when said multiplexing means includes said digital image information within said frame information further.
[Claim 11] Said multiplexing means is a sending set according to claim 10 characterized by generating the voice enable signal which shows transmission of said digitized voice information in said vertical-retrace-line period where said digitized voice information is multiplexed, and/or said horizontal blanking interval.
[Claim 12] It is the sending set according to claim 3 which said multiplexing means generates said frame information using the multiplex control signal which identifies transmission of said digitized voice information and said digital image information, and is characterized by said transmitting means transmitting said multiplex control signal.
[Claim 13] Said multiplexing means is a sending set according to claim 3 characterized by keeping a non-signal period between said digitized voice information and said digital

image information, and generating frame information.
[Claim 14] Said frame information enciphered from the sending set according to claim 3 is received and decoded. A receiving means to receive said frame information which is the graphic display device which extracts and displays said digital image information, and was enciphered from the decoded frame information, An extract means to extract digitized voice information from a decode means to decode said enciphered frame information, and said fly-back-line period kept into said decoded frame information, and to extract digital image information from other periods, The graphic display device which displays said extracted digital image information and is characterized by having an output means to change said extracted digitized voice information into a sound signal.
[Claim 15] It is the graphic display device according to claim 14 which said digitized voice information consists of two or more Rhine speech information, and said frame information keeps a vertical-retrace-line period, then a horizontal blanking interval is kept for every Rhine, and said Rhine speech information is multiplexed in said vertical-retrace-line period and/or said horizontal blanking interval including the Rhine image information, and is characterized by said extract means extracting said Rhine speech information from said vertical-retrace-line period and/or said horizontal blanking interval.
[Claim 16] Said decode means is a graphic display device according to claim 15 characterized by to include a frame decode means decode the digitized voice information and the digital image information which are included in said frame information enciphered as a frame key generation means generate the frame key used as a key of decode, using said frame key generated corresponding to frame information, corresponding to frame information.
[Claim 17] A Rhine decode means to decode the Rhine speech information and the Rhine image information that said frame decode means is included in said enciphered frame information using said frame key, Until decode of all the Rhine speech information contained in said frame information enciphered as a renewal means of a key to update said frame key, and Rhine image information is completed To said Rhine decode means, using said updated frame key, control to decode the following Rhine speech information and the following Rhine image information, and said renewal means of a key is received. The graphic display device according to claim 16 characterized by including the loop control means controlled to update said updated frame key again.
[Claim 18] Said frame decode means is a graphic display device according to claim 16 characterized by using the same decode method in decode of said digitized voice information and said digital image information.
[Claim 19] Said Rhine decode means is a graphic display device according to claim 18 which sets up the initial value for voice, sets up the initial value for images which decodes the Rhine speech information, next has the same value as said initial value

for voice using said set-up initial value for voice, and is characterized by decoding the Rhine image information using said set-up initial value for images.
[Claim 20] Said decode means is a graphic display device according to claim 16 characterized by using a common operation module in decode of said frame information as which authentication by said graphic display device and said frame key were generated and enciphered.
[Claim 21] It is the graphic display device according to claim 15 with which said transmitting means receives said voice enable signal which shows further transmission of said image enable signal which shows transmission of said digital image information, and said digitized voice information, and said extract means is characterized by to extract said digitized voice information in the period when said digital image information is extracted at and said voice enable signal shows it in the period when said image enable signal shows within said frame information further.
[Claim 22] It is the graphic display device according to claim 14 which said receiving means receives the multiplex control signal which identifies transmission of said digitized voice information and said digital image information, and is characterized by said extract means extracting said digitized voice information and said digital image information using said multiplex control signal.
[Claim 23] Said receiving means keeps a non-signal period between said digitized voice information and said digital image information, and the enciphered frame information is received. Said extract means In the non-signal period between said digitized voice information and said digital image information The graphic display device according to claim 14 which generates the multiplex control signal which identifies reception of said digitized voice information and said digital image information, and is characterized by extracting said digitized voice information and said digital image information using said generated multiplex control signal.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the code transmission system which

enciphers and transmits a digital video signal and a digital sound signal.

[0002]

[Description of the Prior Art] If the video signal of an analog is transmitted to LCD (Liquid Crystal Display Device) or CRT (Cathode Ray Tube), a blot and a ghost will occur in the display screen by wave-like strain etc.

(DVI specification) In order to solve the above-mentioned problem, by DVI (Digital Visual Interface) specification, the video signal to LCD or CRT is transmitted by digital one. Thereby, the screen of high quality without a transmission strain can be displayed.

[0003] The conventional signal-transmission system by which DVI specification was applied consists of a sending set and a receiving set, and the sending set and the receiving set are connected through the transmission line. A sending set is equipped with three a TMDS encoder / serializers, and a receiving set is equipped with three a TMDS decoder / recovery. Three component signals which consist of RED(s), GREEN(s), and BLUE(s) are inputted into the TMDS encoder / serializer which corresponds, respectively, and each TMDS encoder / serializer carry out TMDS encoding, carries out the Syria rise of each component signal, and sends it out to a transmission line. Next, TMDS decoding is carried out, and each TMDS decoder / recovery of a receiving set recover the received signal, and restores a component signal.

[0004] the signal with which DE (enable [data]) signal shows the period when component signals, such as RED, GREEN, and BLUE, exist -- it is -- HIGH -- it is active. For example, the period when DE signal serves as LOW is the Horizontal Synchronizing signal period or Vertical Synchronizing signal period of an image. CTL0, CTL1, CTL2, and CTL3 are prepared for the CTL signal as a control signal. In addition, by current DVI specification, these signals are in an intact condition. Specifically, the level of a signal is always 0.

[0005] The TMDS encoder / serializer of a sending set carry out the Syria rise of the video signal which changed into 10 bits the video signal inputted by 8 bits, and was changed into 10 bits, and sends it out to a transmission line. The purpose changed into 10 bits from 8 bits is making it the form where lessened the changing point of data and it was suitable for high-speed transmission. Moreover, a TMDS encoder / serializer changes 2 bits of control signals into 10 bits, and sends them out to a transmission line. Moreover, a data enable signal is also doubled, and it encodes, and the Syria rise is carried out and it is sent out to a transmission line. The TMDS decoder / recovery of a receiving set decode the 10-bit serial data received from the transmission line to 2 bits of each of 8 bits of a chrominance signal, a data enable signal, and a control signal, and develops.

[0006] (HDCP specification) HDCP (High-bandwidth Digital Content Protection System) specification is proposed again as a digital content protection system which suited DVI specification. HDCP specification is the specification for transmitting the

image contents for which protection of copyrights is needed using the signal-transmission system which suits DVI specification, and, fundamentally, consists of encryption of a sending set, a receiving set, authentication of a between, a key share, and the image contents on a channel.

[0007] The signal-transmission system which applied HDCP specification has the authentication section which does authentication with a receiving set, and key sharing, the cryptopart which encipher image information using the shared key, and the TMDS coding section, and has the authentication section which does authentication with a sending set, and key sharing, the TMDS decode section, and the decode section which decode using the key which shared the received signal in a receiving set in a sending set.

[0008] By this configuration, it is I2 between a sending set and a receiving set. After carrying out authentication and a key share through C bus, a sending set enciphers image RGB data and transmits them through the TMDS encoder of DVI specification. After receiving through the TMDS decode section of DVI specification, a receiving set decodes the image RGB data enciphered using the same key as a sending set, and obtains the image RGB data of a basis. It is HDCP about the code used by HDCP specification here. Cipher is called and it is HDCP. The part of the core of Cipher is common in authentication, a key share, and an image data encryption.

[0009] As explained above, the image of high quality can be transmitted in the data transmission system which applies DVI specification and HDCP specification, carrying out protection as a work of the image on a transmission line.

[0010]

[Problem(s) to be Solved by the Invention] In recent years, in a personal computer, a digital-broadcasting receiving set, a DVD regenerative apparatus, etc., playback of the digital image to which the digitized voice was added has spread, and it is requested increasingly that high quality is transmitted about voice as well as the above in addition to an image.

[0011] Then, this invention aims at offering the transmission system which can transmit image information and speech information for high quality, a sending set, a receiving set, and a graphic display device, in order to cope with this request.

[0012]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention is a transmission system which consists of a sending set which keeps a fly-back-line period and transmits digital image information, and a receiving set which receives said digital image information, said sending set transmits digitized voice information in said fly-back-line period, and said receiving set is characterized by receiving said digitized voice information in said fly-back-line period.

[0013] Moreover, the sending set which this invention generates the frame information which keeps a fly-back-line period and includes digital image information,

enciphers, and is transmitted, Receive said enciphered frame information, decode and said digital image information is extracted from the decoded frame information. It is the code transmission system which consists of graphic display devices to display. Said sending set The frame information which multiplexes digitized voice information to said frame information in said fly-back-line period and by which said digitized voice information was multiplexed is enciphered, and it transmits. Said graphic display device Said enciphered frame information is received and decoded, said digitized voice information is extracted from said fly-back-line period kept into said frame information which generated and generated frame information, and it is characterized by changing into a sound signal.

[0014] Moreover, this invention is the sending set which generates the frame information which keeps one or more fly-back-line periods, and includes digital image information, enciphers, and transmits, and is characterized by to have a multiplexing means multiplex digitized voice information to said frame information in said fly-back-line period, an encryption means encipher said frame information by which said digitized voice information was multiplexed, and a transmitting means transmit said enciphered frame information.

[0015] Here, said generated frame information keeps a vertical-retrace-line period, then a horizontal blanking interval is kept for every Rhine, and including the Rhine image information, said digitized voice information consists of two or more Rhine speech information, and said multiplexing means may be constituted so that said Rhine speech information may be multiplexed in said vertical-retrace-line period and/or said horizontal blanking interval.

[0016] Here, said encryption means may be constituted so that a frame key generation means to generate the frame key used as a key of encryption, and the frame cryptographer stage which enciphers the digitized voice information and digital image information which are included in said frame information using said frame key generated corresponding to frame information may be included corresponding to frame information.

[0017] The Rhine cryptographer stage which enciphers the Rhine speech information and the Rhine image information that said frame cryptographer stage is included in said frame information using said frame key here, Until encryption of a renewal means of a key to update said frame key, all the Rhine speech information contained in said frame information, and Rhine image information is completed To said Rhine encryption means, using said updated frame key, control to encipher the following Rhine speech information and the following Rhine image information, and said renewal means of a key is received. You may constitute so that the loop control means controlled to update said updated frame key again may be included.

[0018] Here, in encryption of said digitized voice information and said digital image information, said frame cryptographer stage may be constituted so that the same

cipher system may be used. Here, said Rhine cryptographer stage sets up the initial value for voice, and using said set-up initial value for voice, it may set up the initial value for images which enciphers the Rhine speech information, next has the same value as said initial value for voice, and using said set-up initial value for images, it may constitute it so that the Rhine image information may be enciphered.

[0019] Here, said sending set may transmit said enciphered frame information to a graphic display device, and in authentication of said graphic display device, generation of said frame key, and encryption of said frame information, said encryption means may be constituted so that a common operation module may be used. Here, the image enable signal which shows transmission of said digital image information in the period when said multiplexing means includes said digital image information within said frame information further is generated, and in said fly-back-line period, the voice enable signal which shows transmission of said digitized voice information may be generated, and further, said transmitting means may be constituted so that said generated image enable signal and said voice enable signal may be transmitted.

[0020] Here, in said vertical-retrace-line period where said digitized voice information is multiplexed, and/or said horizontal blanking interval, said multiplexing means may be constituted so that the voice enable signal which shows transmission of said digitized voice information may be generated. Here, said multiplexing means may generate said frame information using the multiplex control signal which identifies transmission of said digitized voice information and said digital image information, and said transmitting means may be constituted so that said multiplex control signal may be transmitted.

[0021] Here, said multiplexing means may be constituted so that a non-signal period may be kept between said digitized voice information and said digital image information and frame information may be generated. Moreover, this invention receives and decodes said frame information enciphered from said sending set. A receiving means to receive said frame information which is the graphic display device which extracts and displays said digital image information, and was enciphered from the decoded frame information, An extract means to extract digitized voice information from a decode means to decode said enciphered frame information, and said fly-back-line period kept into said decoded frame information, and to extract digital image information from other periods, Said extracted digital image information is displayed and it is characterized by having an output means to change said extracted digitized voice information into a sound signal.

[0022] Here, said digitized voice information consists of two or more Rhine speech information, and said frame information keeps a vertical-retrace-line period, then said Rhine speech information is multiplexed in said vertical-retrace-line period and/or said horizontal blanking interval including the Rhine image information by keeping a horizontal blanking interval for every Rhine, and said extract means may be

constituted so that said Rhine speech information may be extracted from said vertical-retrace-line period and/or said horizontal blanking interval.

[0023] Here, said decode means may be constituted so that a frame decode means decode the digitized voice information and the digital image information which are included in said frame information enciphered as a frame key generation means to generate the frame key used as a key of decode, using said frame key generated corresponding to frame information may be included corresponding to frame information.

[0024] A Rhine decode means to decode the Rhine speech information and the Rhine image information that said frame decode means is included in said enciphered frame information here using said frame key, Until decode of all the Rhine speech information contained in said frame information enciphered as a renewal means of a key to update said frame key, and Rhine image information is completed To said Rhine decode means, using said updated frame key, control to decode the following Rhine speech information and the following Rhine image information, and said renewal means of a key is received. You may constitute so that the loop control means controlled to update said updated frame key again may be included.

[0025] Here, in decode of said digitized voice information and said digital image information, said frame decode means may be constituted so that the same decode method may be used. Here, said Rhine decode means sets up the initial value for voice, and using said set-up initial value for voice, it may set up the initial value for images which decodes the Rhine speech information, next has the same value as said initial value for voice, and using said set-up initial value for images, it may constitute it so that the Rhine image information may be decoded.

[0026] Here, in decode of said frame information as which authentication by said graphic display device and said frame key were generated and enciphered, said decode means may be constituted so that a common operation module may be used. Here, said transmitting means may receive said voice enable signal which shows further transmission of said image enable signal which shows transmission of said digital image information, and said digitized voice information, and said extract means may be constituted so that said digital image information may be further extracted in the period which said image enable signal shows within said frame information and said digitized voice information may be extracted in the period which said voice enable signal shows.

[0027] Here, said receiving means may receive the multiplex control signal which identifies transmission of said digitized voice information and said digital image information, and using said multiplex control signal, said extract means may be constituted so that said digitized voice information and said digital image information may be extracted. Said receiving means keeps a non-signal period between said digitized voice information and said digital image information, and the enciphered

frame information is received here. Said extract means In the non-signal period between said digitized voice information and said digital image information The multiplex control signal which identifies reception of said digitized voice information and said digital image information may be generated, and using said generated multiplex control signal, you may constitute so that said digitized voice information and said digital image information may be extracted.

[0028]

[Embodiment of the Invention] The personal computer system 10 as a gestalt of operation of one concerning this invention is explained.

1. The configuration personal computer system 10 of the personal computer system 10 consists of the PC (personal computer) main frame 20, a CRT display unit 30, a keyboard 41, and a mouse 42, as shown in drawing 1 . The PC main frame 20 and the CRT display unit 30 are connected by Cables 50a and 50b.

[0029] Moreover, the PC main frame 20 consists of units which are not illustrating the video connection 201, the image speech processing section 202, the DVD I/O section 203, a control section 204, and others, as shown in drawing 2 . Moreover, as for the PC main frame 20, the computer program is memorized by said RAM or said hard disk unit including a microprocessor, ROM and RAM, a hard disk unit, etc. When said microprocessor operates according to said computer program, the PC main frame 20 attains the function.

[0030] The CRT display unit 30 is constituted including the video connection 301, the display control section 302, the CRT section 303, the loudspeaker control section 304, and the loudspeaker 305. The video connection 201 consists of the multiplex section 211, a HDCP cryptopart 215, and the TMDS coding section 213, as shown in drawing 3 . The HDCP cryptopart 215 contains a cryptopart 212 and the authentication key share section 214. Moreover, the video connection 301 consists of the TMDS decode section 311, the HDCP decode section 315, and the separation section 313, as shown in drawing 3 . The HDCP decode section 315 contains a cryptopart 312 and the authentication key share section 314.

[0031] DVD is recording the coding image speech information which consists of coding image information that compression coding of the image information was carried out, and coding speech information by which compression coding of the speech information was carried out. An example of said image speech information is movie information which consists of a dynamic image and speech information. The DVD I/O section 203 is equipped with said DVD by the user. From DVD with which the PC main frame 20 was equipped, the PC main frame 20 reads coding image speech information, separates the read coding image speech information, and generates coding image information and coding speech information. Next, coding image information is decoded and decode image information is generated. Here, decode image information and coding speech information are digital signals. Next, the PC main

frame 20 enciphers decode image information and coding speech information, respectively, and outputs the encryption image information and encryption speech information which generated and generated encryption image information and encryption speech information to the CRT display unit 30 through cable 50a. The CRT display unit 30 decodes reception, and the received encryption image information and encryption speech information for encryption image information and encryption speech information, displays the decode image information which generated and generated decode image information and decode speech information on the CRT section 303, changes the generated decode speech information into the sound signal of an analog, and outputs it by the loudspeaker 305.

[0032] 1.1 Keyboard 41, mouse 42, control-section 204, DVD I/O section 203, and image speech processing section 202 keyboard 41 and a mouse 42 generate the directions information corresponding to the directions which received the input of the directions which reproduce said coding image speech information currently recorded on said DVD, and received the input from the user, and output the generated directions information to a control section 204.

[0033] A control section 204 outputs read-out directions of said coding image speech information for said directions information to the DVD I/O section 203 based on reception and the received directions information. The DVD I/O section 203 outputs said coding image speech information which read said coding image speech information from said DVD, and read the aforementioned read-out directions based on reception and the received read-out directions to the image speech processing section 202.

[0034] The image speech processing section 202 separates reception and said received coding image speech information for said coding image speech information, decodes the coding image information which generated and generated coding image information and coding speech information, and outputs the decode image information which generated and generated decode image information, and the generated coding speech information to the video connection 201.

1.2 The video connection 201(1) multiplex section 211 multiplex section 211 receives decode image information and coding speech information from the image speech processing section 202.

[0035] Decode image information includes two or more frame image information equivalent to one frame. By displaying said two or more frame image information continuously, a dynamic image is expressed in the CRT display unit 30. Moreover, each frame image information includes 480 Rhine image information equivalent to one line. Moreover, coding speech information contains the frame speech information corresponding to said frame image information. Frame speech information is changed and outputted to voice within the time zone when the frame image information that it corresponds is reproduced in the CRT display unit 30. Moreover, each frame speech

information contains 480 Rhine speech information corresponding to said Rhine image information.

[0036] The multiplex section 211 establishes the vertical-retrace-line period containing the time of day when the Vertical Synchronizing signal of a predetermined number individual is transmitted just before said frame image information is transmitted, in order to establish the synchronization for displaying said frame image information between the PC main frame 20 and the CRT display unit 30, in case one frame image information is transmitted to the CRT display unit 30 from the PC main frame 20 among said decode image information. Next, in order to establish the synchronization for displaying each Rhine image information within one frame image information, the horizontal blanking interval containing the time of day when a Horizontal Synchronizing signal is transmitted just before each Rhine image information is transmitted is prepared.

[0037] The relation between a vertical-retrace-line period, a horizontal blanking interval, and one frame image information is shown in drawing 4 . As shown in this drawing, each frame image information shall consist of 480 Rhine image information, and each Rhine image information shall consist of 720 pixels. Moreover, each pixel consists of 24 bits and each pixel includes RED, GREEN, and 8 bits of component information for BLUE at a time, respectively. As shown in this drawing, the multiplex section 211 prepares the time zone which is equivalent to transmission of 45 Rhine image information just before transmitting one frame image information as a vertical-retrace-line period. Next, the time zone which is equivalent to transmission of 138 pixels just before transmitting each Rhine image information is prepared as a horizontal blanking interval.

[0038] The multiplex section 211 outputs the data enable signals DE and ADE which set data enable signal DE for video signals as LOW at the initiation time of said vertical-retrace-line period, set data enable signal ADE for sound signals as LOW, and were set as LOW about one frame image information among the received decode image information to the TMDS coding section 213, as shown in drawing 5 .

[0039] Next, when the HDCP cryptopart 215 completes count of a frame key so that it may mention later within said vertical-retrace-line period, data enable signal ADE which set data enable signal ADE for sound signals as HIGH from this time, and was set as HIGH is outputted to the TMDS coding section 213. Moreover, the output of coding speech information is started from this time.

[0040] Drawing 5 shows the temporal response of the data enable signals DE and ADE within the time zone when one frame image information is transmitted, decode image information, and coding speech information. In this drawing, time amount passes toward a right end since the left end in Rhine 401. Then, it passes toward a right end since the left end in Rhine 402. In the following and Rhine 403, 404, ..., 405, it is the same.

[0041] The time zone which Rhine 401, 402, ..., 403 shows is said vertical-retrace-line period. In the time zone which Rhine 401 shows, the multiplex section 211 sets data enable signal DE as LOW, and sets data enable signal ADE as LOW. Moreover, in this time zone, decode image information and coding speech information are not outputted. Moreover, in the initiation time of the time zone which Rhine 401 shows, count of the frame key by the HDCP cryptopart 215 is started.

[0042] The multiplex section 211 sets the data enable signals DE and ADE as LOW like the above at the initiation time of the time zone which Rhine 402 shows. Next, supposing count of the frame key by the HDCP cryptopart 215 mentioned above within the time zone which Rhine 402 shows is completed, data enable signal ADE which set data enable signal ADE for sound signals as HIGH from this completion time, and was set as HIGH will be outputted to the TMDS coding section 213. Moreover, the output of one voice image information is started from this time.

[0043] In the time zone which from next Rhine in Rhine 402 to Rhine 403 shows, the multiplex section 211 sets data enable signal DE as LOW, sets data enable signal ADE for sound signals as HIGH, and outputs the data enable signals DE and ADE to the TMDS coding section 213. Moreover, it continues, and said one Rhine image information is outputting the multiplex section 211, and it is continued.

[0044] Next, in the time zone which Rhine 404 shows, the multiplex section 211 outputs data enable signal DE which set data enable signal DE as LOW, and was set as LOW to the TMDS coding section 213 within the time zone equivalent to a horizontal blanking interval. Next, about the period of one Rhine image information which begins from immediately after termination of a horizontal blanking interval, the multiplex section 211 outputs data enable signal DE which set data enable signal DE as HIGH, and was set as HIGH to the TMDS coding section 213.

[0045] Moreover, in the time zone which Rhine 404 shows, in a horizontal blanking interval, the multiplex section 211 sets up and outputs data enable signal ADE for sound signals to HIGH, continues said one Rhine speech information, and outputs it to a cryptopart 212. Here, one Rhine speech information continued and outputted in Rhine 402 – Rhine 404 consists of voice cels of the number which becomes settled by the time of the HDCP cryptopart 215 completing count of a frame key. Each voice cel consists of coding speech information of 24 bit length. Moreover, the multiplex section 211 outputs one Rhine image information to a cryptopart 212 in the period of one Rhine image information which begins from immediately after termination of a horizontal blanking interval. One Rhine image information consists of 720 pixels.

[0046] The relation of the data enable signals DE and ADE within each time zone which from next Rhine in Rhine 404 to Rhine 405 shows to drawing 6 , coding speech information, and decode image information is shown. As shown in this drawing, the multiplex section 211 outputs one Rhine speech information to a cryptopart 212 in a horizontal blanking interval. Here, one Rhine speech information consists of 138 voice

cels. Each voice cel consists of coding speech information of 24 bit length. Moreover, the multiplex section 211 outputs one Rhine image information to a cryptopart 212 in the period of one Rhine image information which begins from immediately after termination of a horizontal blanking interval. One Rhine image information consists of 720 pixels.

[0047] Moreover, the multiplex section 211 outputs said Vertical Synchronizing signal VSYNC which generated and generated Vertical Synchronizing signal VSYNC of said predetermined number individual within the vertical-retrace-line period to the TMDS coding section 213. Moreover, Horizontal Synchronizing signal HSYNC which generated and generated Horizontal Synchronizing signal HSYNC within the horizontal blanking interval is outputted to the TMDS coding section 213.

[0048] (2) The authentication key share section 214 authentication key share section 214 operates according to HDCP specification. Main actuation of the authentication key share section 214 is generation of the random number for the device authentication between the authentication key share section 214 and the equipment of a receiving side, a key share, and encryption etc. About the detail of the authentication key share section 214, since it is specified to HDCP specification, explanation is omitted.

[0049] The authentication key share section 214 is I2. It connects with the authentication key share section 314 mentioned later through cable 50b which is C bus. In addition, it mentions later about a characteristic function, a characteristic configuration, etc. of the authentication key share section 214 in the gestalt of this operation.

(3) Cryptopart 212 cryptopart 212 receives the authentication key share section 214 to reception and the random number PRj for a pixel and a voice cel from the multiplex section 211 for every clock of operation.

[0050] Next, when a pixel is received, as shown in a formula 1, a cryptopart 212 gives an exclusive OR to the pixel and random number PRj which were received for every bit, and outputs the encryption pixel which generated and generated the encryption pixel to the TMDS coding section 213.

(Formula 1) encryption pixel = -- the pixel (+) random number PRj -- here, a operator (+) shows an exclusive OR.

[0051] Moreover, when a voice cel is received, as shown in a formula 2, similarly, a cryptopart 212 gives an exclusive OR to the voice cel and random number PRj which were received for every bit, and outputs the encryption voice cel which generated and generated the encryption voice cel to the TMDS coding section 213.

(Formula 2) The encryption voice cel = voice cel (+) random-number PRj(4) TMDS coding section 213TMDS coding section 213 is connected with the TMDS decode section 311 mentioned later through cable 50a.

[0052] The TMDS coding section 213 consists of TMDS encoder serializers 213a,

213b, and 213c, as shown in drawing 7 . The TMDS encoder serializers 213a, 213b, and 213c are connected with the TMDS decoder recovery 311a, 311b, and 311c mentioned later through the channels C12, C11, and C10 in cable 50a, respectively, as shown in this drawing.

[0053] (TMDS encoder serializer 213a) TMDS encoder serializer 213a receives the component information on RED of the encryption pixels, and 8 bits of heads of a voice cel from a cryptopart 212. Moreover, the control signal of data enable signal DE for video signals, data enable signal ADE for sound signals, and others is received from the multiplex section 211.

[0054] TMDS encoder serializer 213a carries out TMDS encoding, carries out the Syria rise of the control signal of the component information on received 8-bit RED and 8 bits [23:16] of heads of a voice cel, data enable signal DE, data enable signal ADE, and others, and sends it out to TMDS decoder recovery 311a through a channel C12.

[0055] TMDS encoder serializer 213a changes the component information on 8-bit RED, and 8 bits [23:16] of heads of a voice cel into 10-bit information, respectively, carries out the Syria rise of the 10-bit information, and, specifically, sends it out. It changes into 10 bits from 8 bits for making it the form where lessened the changing point of data by this conversion, and it was suitable for high-speed transmission. Moreover, TMDS encoder serializer 213a changes and sends out the data enable signals DE and ADE which are 2-bit control signals to 10 bits.

[0056] (TMDS encoder serializer 213b) TMDS encoder serializer 213b receives the component information on GREEN of the encryption pixels, and 8 bits [15:8] of centers of a voice cel from a cryptopart 212. Moreover, the control signal of data enable signal DE for video signals and others is received from the multiplex section 211.

[0057] Like the above, TMDS encoder serializer 213b carries out TMDS encoding, carries out the Syria rise of the control signal of the component information on received GREEN, 8 bits [15:8] of centers of a voice cel, data enable signal DE, and others, and sends it out to TMDS decoder recovery 311b through a channel C11.

[0058] (TMDS encoder serializer 213c) TMDS encoder serializer 213c receives the component information on BLUE of the encryption pixels, and 8 bits [0:7] of tails of a voice cel from a cryptopart 212. Moreover, data enable signal DE for video signals, Vertical Synchronizing signal VSYNC, and Horizontal Synchronizing signal HSYNC are received from the multiplex section 211.

[0059] Like the above, TMDS encoder serializer 213c carries out TMDS encoding, carries out the Syria rise of the component information on received BLUE, 8 bits [0:7] of tails of a voice cel, data enable signal DE, Vertical Synchronizing signal VSYNC, and Horizontal Synchronizing signal HSYNC, and sends them out to TMDS decoder recovery 311c through a channel C10.

[0060] 1.3 The video connection 301(1) TMDS decode section 311TMDS decode section 311 consists of TMDS decoder recovery 311a, 311b, and 311c, as shown in drawing 7 .

(TMDS decoder recovery 311a) TMDS decoder recovery 311a A channel C12 is minded. Serial data from the TMDS coding section 213 Reception, The component information on the received serial data to 8 bits RED, 8 bits [23:16] of heads of a voice cel, data enable signal DE, Decode the control signal of data enable signal ADE and others, and the component information on RED and 8 bits [23:16] of heads of a voice cel are outputted to a cryptopart 312. ********** of data enable signal DE, data enable signal ADE, and others is outputted to the separation section 313.

[0061] (TMDS decoder recovery 311b) Through a channel C11, TMDS decoder recovery 311b decodes the component information on reception and the received serial data to GREEN, and 8 bits [15:8] of centers of a voice cel for serial data from the TMDS coding section 213, and outputs the component information on GREEN, and 8 bits [15:8] of centers of a voice cel to a cryptopart 312.

[0062] (TMDS decoder recovery 311c) Through a channel C10, TMDS decoder recovery 311c decodes reception, the component information on the received serial data to BLUE, 8 bits [7:0] of tails of a voice cel, Vertical Synchronizing signal VSYNC, and Horizontal Synchronizing signal HSYNC for serial data from the TMDS coding section 213, outputs the component information on BLUE, and 8 bits [7:0] of tails of a voice cel to a cryptopart 312, and outputs Vertical Synchronizing signal VSYNC and Horizontal Synchronizing signal HSYNC to the display control section 302.

[0063] (2) The authentication key share section 314 authentication key share section 314 operates like the authentication key share section 214 according to HDCP specification. Main actuation of the authentication key share section 314 is generation of the random number for the device authentication between the authentication key share section 314 and the equipment of a transmitting side, a key share, and encryption etc. About the detail of the authentication key share section 314, since it is specified to HDCP specification, explanation is omitted.

[0064] In addition, it mentions later about a characteristic function, a characteristic configuration, etc. of the authentication key share section 314 in the gestalt of this operation.

(3) Cryptopart 312 cryptopart 312 operates like a cryptopart 212. A cryptopart 312 receives the authentication key share section 314 to reception and the random number PRj for an encryption pixel and an encryption voice cel from the TMDS decode section 311 for every clock of operation.

[0065] Next, when an encryption pixel is received, as shown in a formula 3, a cryptopart 312 gives an exclusive OR to the encryption pixel and random number PRj which were received for every bit, and outputs the decode pixel which generated and generated the decode pixel to the separation section 313.

(Formula 3) decode pixel = -- the encryption pixel (+) random number PRj -- here, in a formula 1, since it has a value with same random number used when an encryption pixel was generated and random number used in the formula 3 when a decode pixel was generated, the original pixel is decoded.

[0066] Moreover, when an encryption voice cel is received, as shown in a formula 4, similarly, a cryptopart 312 gives an exclusive OR to the encryption voice cel and random number PRj which were received for every bit, and outputs the decode voice cel which generated and generated the decode voice cel to the separation section 313.

(Formula 4) decode voice cel = -- the encryption voice cel (+) random number PRj -- here, in a formula 2, since it has a value with same random number used when an encryption voice cel was generated and random number used in the formula 4 when a decode voice cel was generated, the original voice cel is decoded.

[0067] (4) The separation section 313 separation section 313 receives data enable signal DE from reception and the TMDS decode section 311, and data enable signal ADE for the information on 24 bit length from a cryptopart 312 for every clock of operation. When received data enable signal DE is HIGH, the separation section 313 considers that the information on received 24 bit length is a decode pixel, and is outputted to the display control section 302 for every clock of operation by making information on received 24 bit length into a decode pixel. Moreover, the separation section 313 outputs received data enable signal DE to the display control section 302.

[0068] Moreover, when received data enable signal ADE is HIGH, the separation section 313 considers that the information on received 24 bit length is a decode voice cel, and is outputted to the loudspeaker control section 304 for every clock of operation by using information on received 24 bit length as a decode voice cel. Moreover, the separation section 313 outputs received data enable signal ADE to the loudspeaker control section 304.

[0069] 1.4 The display control section 302 and the CRT section 303 display control section 302 receive reception and the TMDS decode section 311 to Vertical Synchronizing signal VSYNC and Horizontal Synchronizing signal HSYNC for a decode pixel and data enable signal DE from the separation section 313 for every clock of operation. The display control section 302 outputs each analog signal which generated and generated the analog signal of RED, GREEN, and BLUE to the CRT section 303 based on the decode pixel received for every clock of operation, data enable signal DE, Vertical Synchronizing signal VSYNC, and Horizontal Synchronizing signal HSYNC.

[0070] The CRT section 303 displays reception and the image of a color for the analog signal of RED, GREEN, and BLUE from the display control section 302.

1.5 The loudspeaker control section 304 and the loudspeaker 305 loudspeaker control section 304 decode the decode voice cel with which reception and received data enable signal ADE received a decode voice cel and data enable signal ADE from the separation section 313 between HIGH(s) for every clock of operation, change the

speech information which generated and generated speech information, and output the analog signal which generated and generated the analog signal to a loudspeaker 305.

[0071] A loudspeaker 305 changes reception and the received analog signal for an analog signal from the loudspeaker control section 304, and generates and outputs voice.

2. Explain actuation of the personal computer system 10 of the personal computer system 10 of operation.

(1) Directions of the outline actuation user of the personal computer system 10 explain outline actuation of the personal computer system 10 in the case of reproducing the coding image speech information currently recorded on DVD using the flow chart shown in drawing 8 .

[0072] When it attests whether the PC main frame 20 is equipment with the just CRT display unit 30 between the PC main frame 20 and the CRT display unit 30 (step S101) and authentication fails in it between based on HDCP specification, (step S102) and processing are ended. When authentication is successful, a KSV list is generated based on (step S102) and HDCP specification (step S103). Here, since generation of a KSV list is indicated by HDCP specification, explanation is omitted.

[0073] Next, the value of 0 is set as the variable i which shows the number of a frame (step S104). Next, in S112, the processing shown in S111 from step S105 is repeated for every frame from step S105. The value of 1 is added to Variable i (step S106), and key sharing for every frame is done (step S107). Next, in S111, step S109 to S110 is repeated for every Rhine from step S108.

[0074] Encryption of one Rhine speech information and one Rhine image information, transmission, and decode are performed (step S109), and a key is updated based on HDCP specification (step S110).

(2) Explain actuation of the equipment authentication shown in step S101 of drawing 8 of equipment authentication of operation using the flow chart shown in drawing 9 . In addition, since equipment authentication is indicated by HDCP specification, detailed explanation is omitted.

[0075] The authentication key share section 214 generates An (step S171), and is An and Aksv I2 It transmits to the authentication key share section 314 through cable 50b which is C bus (step S172). The authentication key share section 314 is Bksv and REPEATER I2 It transmits to the authentication key share section 214 through cable 50b which is C bus (step S173).

[0076] The authentication key share section 214 is Km=Akeys. over Bksv is computed (step S174) and =(Ks, M0, and R0) dviBlkCipher (km, REPEATER||An) is computed (step S175). The authentication key share section 314 computes Km'=Bkeys over Aksv (step S176), computes =(Ks', M0', R0') dviBlkCipher (km', REPEATER||An) (step S177), and is R0' I2 It transmits to the authentication key share section 214 through

cable 50b which is C bus (step S178).

[0077] The authentication key share section 214 is R0. R0' is compared, and in being in agreement, (step S179) and the CRT display unit 30 attest with it being just equipment. Moreover, in not being in agreement, (step S179) and the CRT display unit 30 attest with it not being just equipment. (3) Explain the actuation key shared [for every frame] shown in step S107 of drawing 8 [key shared / for every frame] of operation using the flow chart shown in drawing 10 . In addition, since the key share for every frame is indicated by HDCP specification, detailed explanation is omitted.

[0078] The authentication key share section 214 computes =(Ki, Mi, Ri) dviBlkCipher (Ks and REPEATER||Mi-1) (step S131). Next, the authentication key share section 214 computes Ri=ri, only when (i mod 128) is 0 (step S132) (step S133). The authentication key share section 314 computes =(Ki', Mi', Ri') dviBlkCipher (Ks' and REPEATER||M'i -1) (step S141). Next, the authentication key share section 314 computes Ri'=ri', only when (i mod 128) is 0 (step S142) (step S143). Next, the authentication key share section 314 attests with the authentication key share section 214 which transmits Ri' to the authentication key share section 214 through cable 50b which is I2 C bus being equipment with (step S135) and the CRT display unit 30 just when Ri and Ri' is compared every 2 seconds and it is in agreement every 2 seconds. Moreover, in not being in agreement, (step S135) and the CRT display unit 30 attest with it not being just equipment.

[0079] (4) Explain encryption of the one Rhine speech information and one Rhine image information which are shown in step S109 of drawing 8 of encryption of one Rhine speech information and one Rhine image information, transmission, and decode of operation, transmission, and actuation of decode using the flow chart shown in drawing 11 .

[0080] The authentication key share section 214 once memorizes the initial value used in the case of the random-number generation specified in HDCP specification as preservation initial value. here -- said initial value -- concrete -- Mi-1 it is . (Step S200) . Next, in step S201 - step S205, the following steps S202-S204 are repeated about each voice cel ACj in one Rhine speech information. Here, 138 voice cels are contained in one Rhine speech information. Variable j takes the value of 1-138 in the above-mentioned repeat.

[0081] The authentication key share section 214 generates the 24-bit random number PRj (step S202), and a cryptopart 212 gives an exclusive OR to the voice cel ACj and a random number PRj, and generates the encryption voice cel EACj (step S203). Next, a cryptopart 212 transmits the generated encryption voice cel EACj to a cryptopart 312 through the TMDS coding section 213, cable 50a, and the TMDS decode section 311 (step S204).

[0082] The authentication key share section 314 once memorizes the initial value used in the case of the random-number generation specified in HDCP specification as

preservation initial value. here -- said initial value -- concrete -- M'i -1 it is . (Step S221) . Next, in step S222 - step S225, the following steps S223, S204, and S224 are repeated about each encryption voice cel DACj in one Rhine speech information. Here, 138 encryption voice cels are contained in one Rhine speech information. Variable j takes the value of 1-138 in the above-mentioned repeat.

[0083] The authentication key share section 314 generates the 24-bit random number PRj (step S223), a cryptopart 312 gives an exclusive OR to the encryption voice cel DACj and a random number PRj, and generates the decode voice cel DACj, and a cryptopart 312 outputs the decode voice cel DACj generated to the separation section 313 (step S224). The authentication key share section 214 restores said initial value from said once memorized preservation initial value (step S206). Next, in steps S207-S211, the following steps S208-S210 are repeated about each pixel PCj within one Rhine image information. Here, 720 pixels are contained in one Rhine image information. Variable j takes the value of 1-720 in the above-mentioned repeat.

[0084] The authentication key share section 214 generates the 24-bit random number PRj (step S208), a cryptopart 212 gives an exclusive OR to Pixel PCj and the generated random number PRj, and generates the encryption pixel EPCj (step S209), and a cryptopart 212 transmits the generated encryption pixel EPCj to a cryptopart 312 through the TMDS coding section 213, cable 50a, and the TMDS decode section 311 (step S210).

[0085] The authentication key share section 314 restores said initial value from said once memorized preservation initial value (step S226). Next, in steps S227-S230, the following steps S228, S210, and S229 are repeated about each encryption pixel DPCj within one Rhine image information. Here, 720 encryption pixels are contained in one Rhine image information. Variable j takes the value of 1-720 in the above-mentioned repeat.

[0086] The 24-bit random number PRj is generated (step S228), a cryptopart 312 gives an exclusive OR to the encryption pixel DPCj and the generated random number PRj, and the authentication key share section 314 outputs the decode pixel DPCj which generated and generated the decode pixel DPCj to the separation section 313 (step S229).

(5) Explain the state transition of the encryption [decode] by the state-transition HDCP cryptopart 215 [the HDCP decode section 315] of the encryption [decode] by the HDCP cryptopart 215 [the HDCP decode section 315] using drawing 12 . in addition -- here -- [--] -- the inner publication shows the state transition of the decode by the HDCP decode section 315.

[0087] (Transition to an idle state D0 from which condition) When it is in a Reset condition (step S301), or when authentication goes wrong, (step S304) and the HDCP cryptopart 215 [the HDCP decode section 315] change to an idle state D0.

(Transition to the frame key count condition D1 from an idle state D0) The HDCP

cryptopart 215 [the HDCP decode section 315] uses CTL3 intact signal for the synchronizing signal of frame key count by DVI specification based on HDCP specification. It is a time of authentication being successful, and when CTL3 signal of a DVI interface is generated, (step S302) and the HDCP cryptopart 215 [the HDCP decode section 315] change in the frame key count condition D1 of performing frame key count. In the frame key count condition D1, the HDCP cryptopart 215 [the HDCP decode section 315] calculates the frame key used for encryption [decode] of the following image frame.

[0088] (Transition to the image encryption [decode] condition D2 from the frame key count condition D1) If DE signal which gives the head of the video signal which should be encryption [decode] Carried out is received when there is no start signal of a sound signal during V blank period (step S309), the HDCP cryptopart 215 [the HDCP decode section 315] will change in the image encryption [decode] condition D2. In the image encryption [decode] condition D2, the HDCP cryptopart 215 [the HDCP decode section 315] enciphers a video signal [decode].

[0089] (Transition to the Unknown Blank condition D3 from the image encryption [decode] condition D2) The end (generally they are the last of a line or the last of a frame) of a video signal is notified by DE. In drawing 12 , this signal is expressed as "!DE." ! If DE is received (step S308), the HDCP cryptopart 215 [the HDCP decode section 315] will change in the Unknown Blank condition D3. In the Unknown Blank condition D3, the HDCP cryptopart 215 [the HDCP decode section 315] begins renewal of a key.

[0090] (Transition to the frame key count condition D1 from the Unknown Blank condition D3) In the Unknown Blank condition D3, if CTL3 signal is received (step S303), the HDCP cryptopart 215 [the HDCP decode section 315] will change to the frame key count condition D1 of performing new image frame key count. (Transition to H blank condition D4 from the Unknown Blank condition D3) Hsync shows that it is H blank (generally spacing). If Hsync is received (step S310), the HDCP cryptopart 215 [the HDCP decode section 315] will change to H blank condition D4.

[0091] In H blank condition D4, if renewal of a key does not carry out Unknown Blank condition completion by D3, it waits for the HDCP cryptopart 215 [the HDCP decode section 315] here. (Transition to V blank condition D5 from the Unknown Blank condition D3) Vsync shows that it is V blank (generally inter-frame). If Vsync is received (step S318), the HDCP cryptopart 215 [the HDCP decode section 315] will change to V blank condition D5.

[0092] (Transition to the image encryption [decode] condition D2 from H blank condition D4) If DE signal is received when there is no sound signal in H blanking period (step S314), the HDCP cryptopart 215 [the HDCP decode section 315] will begin to encipher the next line of a video signal [decode], and will change to the image encryption [decode] condition D2.

(Transition to the frame key count condition D1 from H blank condition D4) If CTL3 signal occurs (step S315), the HDCP cryptopart 215 [the HDCP decode section 315] will change to the frame key count condition D1 of performing new frame key count.

[0093] (Transition to V blank condition D5 from H blank condition D4) Vsync -- V -- it turns out that it is blank. If Vsync is received (step S316), the HDCP cryptopart 215 [the HDCP decode section 315] will change to V blank condition D5. In V blank condition D5, the HDCP cryptopart 215 [the HDCP decode section 315] waits for a terminating condition.

[0094] (Transition to the frame key count condition D1 from V blank condition D5) If CTL3 signal occurs (step S317), the HDCP cryptopart 215 [the HDCP decode section 315] will change to the frame key count condition D1 in order to perform new frame key count.

(Transition to an idle state D0 from V blank condition D5) When it returns to a video signal with DE signal before CTL3 signal occurred during V blank period (step S319), the HDCP cryptopart 215 [the HDCP decode section 315] does not perform encryption of the following frame. This happens by authentication failure in a link etc.

[0095] during [V blank period] (Transition to the voice encryption [decode] condition D6 from the frame key count condition D1) If there is a start signal ADE of a sound signal (step S305), the HDCP cryptopart 215 <the HDCP decode section 315> will begin to encipher a sound signal [decode]. In the voice encryption [decode] condition D6, the HDCP cryptopart 215 [the HDCP decode section 315] enciphers a sound signal [decode].

[0096] (Transition to the video-signal waiting state D7 from the voice encryption [decode] condition D6) If the end of a sound signal is notified by ADE (step S306), the HDCP cryptopart 215 [the HDCP decode section 315] will change to the video-signal waiting state D7 which waits for a video signal to start. In drawing 12 , this signal is expressed as "!ADE."

[0097] (Transition to the image encryption [decode] condition D2 from the video-signal waiting state D7) DE signal of a TMDS link gives the head of the video signal which should be encryption [decode] Carried out. If DE signal is received (step S307), the HDCP cryptopart 215 [the HDCP decode section 315] will change to the image encryption [decode] condition D2. (Transition to the voice encryption [decode] condition D8 from H blank condition D4) Reception (step S311) and the HDCP cryptopart 215 [the HDCP decode section 315] change an ADE signal to the voice encryption [decode] condition D8, in order to begin encryption [decode] of the sound signal of the next H blanking period.

[0098] In the voice encryption [decode] condition D8, the HDCP cryptopart 215 [the HDCP decode section 315] enciphers a sound signal [decode]. (Transition to the video-signal waiting state D9 from the voice encryption [decode] condition D8) If the end of a sound signal is notified by ADE (step S312), the HDCP cryptopart 215 [the

HDCP decode section 315] will change to the video-signal waiting state D9.

[0099] In the video-signal waiting state D9, the HDCP cryptopart 215 [the HDCP decode section 315] waits for a video signal to start. (Transition to the image encryption [decode] condition D2 from the video-signal waiting state D9) DE signal of a TMDS link gives the head of the video signal which should be encryption [decode] Carried out. If DE signal is received (step S313), the HDCP cryptopart 215 [the HDCP decode section 315] will change to the image encryption [decode] condition D2.

[0100] 3. According to the gestalt of this operation explained more than the conclusion, carry out Time Division Multiplexing of a video signal and the sound signal, and in a transmitting side, the code transmission system which carries out code transmission carries out multiplex [of the sound signal which carried out time base compaction of the sound signal, and carried out this time base compaction] to the blanking period of a video signal, and carries out code transmission.

[0101] Said code transmission system is set to said transmitting side. Moreover, after authentication of a receiving side, And calculate the key for frames after a Vertical Synchronizing signal, and the sound signal which carried out time amount compression using the calculated key for frames is enciphered. A video signal is enciphered after that, further, a key is updated, the sound signal in which used said updated key and the degree carried out time amount compression after the Horizontal Synchronizing signal is enciphered, and the following video signal is enciphered after that.

[0102] Said code transmission system is set to said receiving side. Moreover, after authentication with a transmitting side, And calculate the key for frames after a Vertical Synchronizing signal, and the sound signal enciphered using the calculated key for frames is decoded. The video signal enciphered after that is decoded, the sound signal with which the key was updated, said updated key was further used after the Horizontal Synchronizing signal, and the degree was enciphered is decoded, and the video signal with which the degree was enciphered after that is decoded.

[0103] Moreover, in said transmitting side, said code transmission system notifies encryption transmission of a sound signal to a receiving side with a sound signal enable signal, notifies encryption transmission of a video signal to a receiving side with a video-signal enable signal, and when there is a sound signal enable signal, a sound signal is decoded, and on the other hand, by said receiving side, when there is a video-signal enable signal, it decodes a video signal.

[0104] thus, the data enable signal (DE signal) of a video signal [in / on said code transmission system and / the conventional example] -- in addition, the data enable signal (ADE signal) of a sound signal is added, and it controls, using this as a multiplex control signal. Since this signal is added, also when there is multiplex [no / of a sound signal], processing corresponding to a transmitting side can be performed by the receiving side.

[0105] Moreover, the same cipher system is used for said code transmission system

in encryption of the video signal in each of said transmitting side and a receiving side, and encryption of a sound signal. Moreover, when said cipher system has an internal state, said code transmission system sets up a certain initial state, enciphers a sound signal, after that, returns the internal state of a cipher system to the initial state of a basis, and enciphers the following video signal.

[0106] HDCP used by HDCP Cipher is the cipher system of the type which has an internal state changed at the same time it holds an internal state and enciphers input data depending on this. In a transmitting side, after saving the internal state of the cipher system in condition D3 time and processing a sound signal (condition D8), it returns to the internal state saved at the time of a condition D9, and encryption processing (condition D2) of the following video signal is carried out. By this, by the receiving side, even if it is the receiver corresponding to HDCP which can process only a video signal, the internal state of a cipher system becomes the same by the transmitting side and receiving side in the time of decoding a video signal (that is, transition of a condition D9 to the condition D2 and transition to a condition D2 from a condition D4), and a HDCP receiver can process a video signal correctly.

[0107] Moreover, a common operation module is used for said code transmission system in the authentication in each of said transmitting side and a receiving side, key count and encryption of a video signal, and audio encryption. Thus, since said code transmission system is carrying out cryptographic algorithm used with a sound signal and a video signal in common, the additional part from the conventional code transmission system is stopped by min. Moreover, mounting scales are reducible like HDCP by that of ****** using an operation module common to authentication, a key share, and encryption.

[0108] Moreover, in said transmitting side, said code transmission system multiplexes said video signal and said sound signal using a multiplex control signal, and, on the other hand, separates this in a receiving side using the multiplex control signal sent from the transmitting side. Moreover, according to the gestalt of this operation, by establishing the non-signal period of the die length decided beforehand between processing of a sound signal, and processing of a video signal, and recognizing this by the receiving side, although the multiplex control signal shall be sent to a receiving side from the transmitting side, though the change of a sound signal and a video signal is performed, it is good. Thus, instead of sending said multiplex control signal to a receiving side from a transmitting side, while being a sound signal and a video signal, a non-signal period is established for changing, and said code transmission system recognizes this by the receiving side, and generates a multiplex control signal.

[0109] As mentioned above, according to the gestalt of this operation, by carrying out the minimum escape of the state transition and mounting scale of HDCP specification, multiplex [of the sound signal which carried out time base compaction not only to the conventional video signal but to the blanking period] can be carried out, and

encryption transmission can be carried out. The change section of a sound signal is added to the conventional HDCP specification, and it changes to the enable signal of a sound signal, and controls by signal. About the case where multiplex [of the sound signal] is not carried out by this control, the same processing as the conventional HDCP specification is possible. In addition, by preparing the non-signal section of the specific die length on a data signal, when the addition of a change signal is difficult, though changed by detecting in a receive section, it is good.

[0110] Moreover, maintaining conventional HDCP specification and upward compatibility, this is extended on specification and mounting at the minimum, and encryption transmission of the sound signal can be carried out with a video signal. Furthermore, also in the receiver according to the conventional HDCP specification, the decode playback of the encryption video signal can be carried out. Moreover, by using the same cipher system as a video signal for encryption of a sound signal, an additional module also serves as min and compact mounting of it is attained. Moreover, after encryption of the sound signal in each Rhine, even if it is the case where the thing of the conventional HDCP specification that the receiver does not support an extended specification by returning the internal state of a cipher system to the initial state in each Rhine, i.e., decode of a video signal, is made, a video signal can be decoded correctly.

[0111] 4. Although this invention has been explained based on the gestalt of the above-mentioned operation, this invention of not being limited [which is the gestalt of other operations] to the gestalt of the above-mentioned operation is natural. It is contained in this invention also when as follows.

(1) According to the gestalt of this operation, although the personal computer realizes, it is not limited to this. the digital image to which the digitized voice was added in the digital-broadcasting receiving set, the DVD regenerative apparatus, etc. -- reproducing -- ****** -- being good .

[0112] (2) Although [according to the gestalt of this operation] coding speech information is transmitted to the video connection 301 from the video connection 201 through all the channels C12, C11, and C10, it is good, though the amount of transmissions of coding speech information is lessened and being transmitted only through 1 in said channel, or two pieces. Moreover, only in a vertical-retrace-line period, although [according to the gestalt of this operation] coding speech information is transmitted to the video connection 301 from the video connection 201 in a vertical-retrace-line period and a horizontal blanking interval, though transmitted, it is good. Moreover, only in a horizontal blanking interval, though transmitted, it is good.

[0113] (3) Though this invention is an approach shown above, it is good. Moreover, though it is the computer program which realizes these approaches by computer, it is good, and it is good though it is the digital signal which consists of said computer

program. Moreover, this invention is good also as what recorded said computer program or said digital signal on the record medium in which computer reading is possible, for example, a flexible disk, a hard disk, CD-ROM, MO and DVD, DVD-ROM, DVD-RAM, semiconductor memory, etc. Moreover, it is good though it is said computer program currently recorded on these record media, or said digital signal.

[0114] Moreover, this invention is good also as what is transmitted via the network where said computer program or said digital signal is used into a telecommunication circuit, wireless, or a wire communication circuit, and it uses the Internet representation. Moreover, this invention is the computer system equipped with a microprocessor and memory, said memory has memorized the above-mentioned computer program, and though said microprocessor operates according to said computer program, it is good.

[0115] moreover, the thing for which said program or said digital signal is recorded on said record medium, and is transported -- or by transporting said program or said digital signal via said network etc., though carried out according to other independent computer systems, it is good.

(4) It is good though the gestalt and the above-mentioned modification of the above-mentioned implementation are combined, respectively.

[0116] (Possibility of use on industry) In a personal computer, an information processing terminal, etc., when outputting an image and voice, it can use. Moreover, in a DVD regenerative apparatus or a digital-broadcasting receiving set, when outputting an image and voice, it can use.

[0117]

[Effect of the Invention] As explained above, this invention is a transmission system which consists of a sending set which keeps a fly-back-line period and transmits digital image information, and a receiving set which receives said digital image information, said sending set transmits digitized voice information in said fly-back-line period, and said receiving set receives said digitized voice information in said fly-back-line period.

[0118] By this, image information and speech information can be transmitted and received for high quality. Moreover, the sending set which this invention generates the frame information which keeps a fly-back-line period and includes digital image information, enciphers, and is transmitted, Receive said enciphered frame information, decode and said digital image information is extracted from the decoded frame information. It is the code transmission system which consists of graphic display devices to display. Said sending set The frame information which multiplexes digitized voice information to said frame information in said fly-back-line period and by which said digitized voice information was multiplexed is enciphered, and it transmits. Said graphic display device Said enciphered frame information is received and decoded, said digitized voice information is extracted from said fly-back-line period kept into

said frame information which generated and generated frame information, and it changes into a sound signal.

[0119] Image information and speech information are transmitted and received for high quality, and protection as a work can be performed by this.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is the external view showing the appearance of the personal computer system 10.

[Drawing 2] Drawing 2 is the block diagram showing the configuration of the personal computer system 10.

[Drawing 3] Drawing 3 is the block diagram showing the configuration of the video connection 201 and the video connection 301.

[Drawing 4] Drawing 4 is the conceptual diagram showing the relation between a vertical-retrace-line period, a horizontal blanking interval, and the image information for one frame.

[Drawing 5] Drawing 5 shows change of the data enable signals DE and ADE equivalent to one accompanying the passage of time, decode image information, and coding speech information.

[Drawing 6] Drawing 6 shows change of the data enable signals DE and ADE equivalent to one line accompanying the passage of time, decode image information, and coding speech information.

[Drawing 7] Drawing 7 is the block diagram showing the configuration of the TMDS coding section 213 and the TMDS decode section 311.

[Drawing 8] Drawing 8 is a flow chart which shows outline actuation of the personal computer system 10 in the case of reproducing coding image speech information.

[Drawing 9] Drawing 9 is a flow chart which shows actuation of equipment authentication.

[Drawing 10] Drawing 10 is a flow chart which shows actuation key shared [for every frame].

[Drawing 11] Drawing 11 is a flow chart which shows encryption of the speech

information in one line, and image information, transmission, and actuation of decode.

[Drawing 12] Drawing 12 is a transition chart which shows the state transition of the encryption [decode] by the HDCP cryptopart 215 [the HDCP decode section 315].

[Description of Notations]

10 Personal Computer System
20 PC Main Frame
30 CRT Display Unit
41 Keyboard
42 Mouse
50a Cable
50b Cable
201 Video Connection
202 Image Speech Processing Section
203 DVD I/O Section
204 control sections
211 Multiplex Section
212 Cryptopart
213 TMDS Coding Section
214 Authentication Key Share Section
215 HDCP Cryptopart
301 Video Connection
302 Display Control Section
303 The CRT Section
304 Loudspeaker Control Section
305 Loudspeaker
311 TMDS Decode Section
312 Cryptopart
313 Separation Section
314 Authentication Key Share Section
315 HDCP Decode Section

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－281464
（P2002－281464A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｎ　7/08		Ｈ０４Ｎ　7/08	１０１	５Ｃ０６３
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３	５Ｊ１０４
Ｈ０４Ｎ　7/081		Ｈ０４Ｎ　7/087		
7/083				
7/087				

審査請求　未請求　請求項の数23　ＯＬ　（全 20 頁）　最終頁に続く

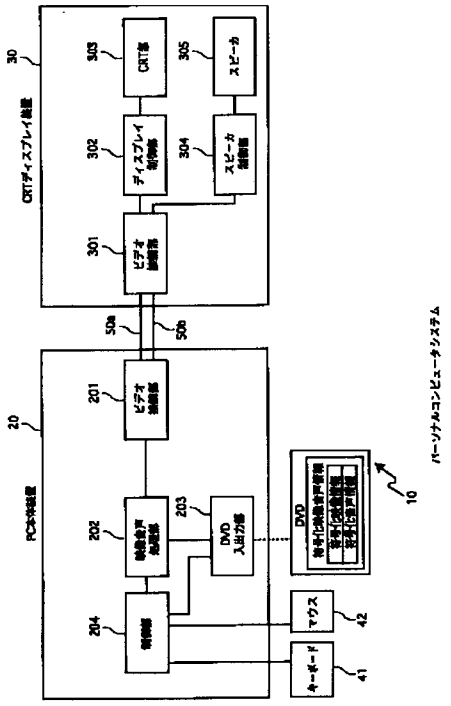
(21)出願番号　特願2001－383577(P2001－383577)
(22)出願日　平成13年12月17日(2001.12.17)
(31)優先権主張番号　特願2000－383345(P2000－383345)
(32)優先日　平成12年12月18日(2000.12.18)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　暗号伝送システム

(57)【要約】
【課題】　パーソナルコンピュータなどにおいて、デジタル音声の付加されたデジタル映像の再生が普及しており、映像に加えて音声についても、高品質の伝送を行うことが要望されるようになってきている。映像情報と音声情報とを高品質で伝送することができる伝送システムを提供する。
【解決手段】映像情報と音声情報とを高品質で伝送する伝送システムは、映像信号と音声信号を時分割多重して暗号伝送する。送信側において、音声信号を時間軸圧縮し、該時間軸圧縮した音声信号を、映像信号のブランキング期間に多重して暗号伝送する。音声信号データイネーブル信号ADEと、音声信号と映像信号の切り替え信号を用いて制御する。



【特許請求の範囲】

【請求項１】　デジタル映像情報を帰線期間を置いて送信する送信装置と、前記デジタル映像情報を受信する受信装置とから構成される伝送システムであって、
前記送信装置は、前記帰線期間においてデジタル音声情報を送信し、
前記受信装置は、前記帰線期間において前記デジタル音声情報を受信することを特徴とする伝送シテスム。

【請求項２】　帰線期間を置いてデジタル映像情報を含むフレーム情報を生成し、暗号化して送信する送信装置と、暗号化された前記フレーム情報を受信して復号し、復号されたフレーム情報から前記デジタル映像情報を抽出し、表示する映像表示装置とから構成される暗号伝送システムであって、
前記送信装置は、デジタル音声情報を前記帰線期間において前記フレーム情報に多重化し、前記デジタル音声情報が多重化されたフレーム情報を暗号化して送信し、
前記映像表示装置は、暗号化された前記フレーム情報を受信し、復号してフレーム情報を生成し、生成した前記フレーム情報内に置かれた前記帰線期間から前記デジタル音声情報を抽出し、音声信号に変換することを特徴とする暗号伝送シテスム。

【請求項３】　１以上の帰線期間を置いてデジタル映像情報を含むフレーム情報を生成し、暗号化して送信する送信装置であって、
デジタル音声情報を前記帰線期間において前記フレーム情報に多重化する多重化手段と、
前記デジタル音声情報が多重化された前記フレーム情報を暗号化する暗号化手段と、
暗号化された前記フレーム情報を送信する送信手段とを備えることを特徴とする送信装置。

【請求項４】　生成された前記フレーム情報は、垂直帰線期間を置き、続いて、ライン毎に、水平帰線期間を置いてライン映像情報を含み、
前記デジタル音声情報は、複数個のライン音声情報から構成され、
前記多重化手段は、前記垂直帰線期間及び／又は前記水平帰線期間において前記ライン音声情報を多重化することを特徴とする請求項３に記載の送信装置。

【請求項５】　前記暗号化手段は、
フレーム情報に対応して、暗号化の鍵として用いられるフレーム鍵を生成するフレーム鍵生成手段と、
フレーム情報に対応して生成された前記フレーム鍵を用いて、前記フレーム情報に含まれるデジタル音声情報及びデジタル映像情報を暗号化するフレーム暗号手段とを含むことを特徴とする請求項４に記載の送信装置。

【請求項６】　前記フレーム暗号手段は、
前記フレーム鍵を用いて、前記フレーム情報に含まれるライン音声情報及びライン映像情報を暗号化するライン暗号手段と、
前記フレーム鍵を更新する鍵更新手段と、
前記フレーム情報に含まれる全てのライン音声情報及びライン映像情報の暗号化が終了するまで、前記ライン暗号化手段に対して、更新された前記フレーム鍵を用いて、次のライン音声情報及び次のライン映像情報を暗号化するように制御し、前記鍵更新手段に対して、更新された前記フレーム鍵を再度更新するように制御する繰返制御手段とを含むことを特徴とする請求項５に記載の送信装置。

【請求項７】　前記フレーム暗号手段は、前記デジタル音声情報及び前記デジタル映像情報の暗号化において、同一の暗号化方式を用いることを特徴とする請求項５に記載の送信装置。

【請求項８】　前記ライン暗号手段は、音声用初期値を設定し、設定した前記音声用初期値を用いて、ライン音声情報を暗号化し、次に、前記音声用初期値と同じ値を有する映像用初期値を設定し、設定した前記映像用初期値を用いて、ライン映像情報を暗号化することを特徴とする請求項７に記載の送信装置。

【請求項９】　前記送信装置は、暗号化された前記フレーム情報を映像表示装置に対して送信し、
前記暗号化手段は、前記映像表示装置の認証、前記フレーム鍵の生成及び前記フレーム情報の暗号化において、共通の演算モジュールを用いることを特徴とする請求項５に記載の送信装置。

【請求項１０】　前記多重化手段は、さらに、前記フレーム情報内で前記デジタル映像情報を含む期間において、前記デジタル映像情報の送信を示す映像イネーブル信号を生成し、前記帰線期間において、前記デジタル音声情報の送信を示す音声イネーブル信号を生成し、
前記送信手段は、さらに、生成された前記映像イネーブル信号及び前記音声イネーブル信号を送信することを特徴とする請求項４に記載の送信装置。

【請求項１１】　前記多重化手段は、前記デジタル音声情報を多重化する前記垂直帰線期間及び／又は前記水平帰線期間において、前記デジタル音声情報の送信を示す音声イネーブル信号を生成することを特徴とする請求項１０に記載の送信装置。

【請求項１２】　前記多重化手段は、前記デジタル音声情報及び前記デジタル映像情報の送信を識別する多重制御信号を用いて、前記フレーム情報を生成し、
前記送信手段は、前記多重制御信号を送信することを特徴とする請求項３に記載の送信装置。

【請求項１３】　前記多重化手段は、前記デジタル音声情報と前記デジタル映像情報との間に無信号期間を置いてフレーム情報を生成することを特徴とする請求項３に記載の送信装置。

【請求項１４】　請求項３に記載の送信装置から暗号化された前記フレーム情報を受信して復号し、復号されたフレーム情報から前記デジタル映像情報を抽出し、表示

する映像表示装置であって、
暗号化された前記フレーム情報を受信する受信手段と、
暗号化された前記フレーム情報を復号する復号手段と、
復号された前記フレーム情報内に置かれた前記帰線期間からデジタル音声情報を抽出し、他の期間からデジタル映像情報を抽出する抽出手段と、
抽出した前記デジタル映像情報を表示し、抽出した前記デジタル音声情報を音声信号に変換する出力手段とを備えることを特徴とする映像表示装置。
【請求項１５】　前記デジタル音声情報は、複数個のライン音声情報から構成されており、
前記フレーム情報は、垂直帰線期間を置き、続いて、ライン毎に、水平帰線期間を置いてライン映像情報を含み、前記垂直帰線期間及び／又は前記水平帰線期間において、前記ライン音声情報が多重化されており、
前記抽出手段は、前記垂直帰線期間及び／又は前記水平帰線期間から前記ライン音声情報を抽出することを特徴とする請求項１４に記載の映像表示装置。
【請求項１６】　前記復号手段は、
フレーム情報に対応して、復号の鍵として用いられるフレーム鍵を生成するフレーム鍵生成手段と、
フレーム情報に対応して生成された前記フレーム鍵を用いて、暗号化された前記フレーム情報に含まれるデジタル音声情報及びデジタル映像情報を復号するフレーム復号手段とを含むことを特徴とする請求項１５に記載の映像表示装置。
【請求項１７】　前記フレーム復号手段は、
前記フレーム鍵を用いて、暗号化された前記フレーム情報に含まれるライン音声情報及びライン映像情報を復号するライン復号手段と、
前記フレーム鍵を更新する鍵更新手段と、
暗号化された前記フレーム情報に含まれる全てのライン音声情報及びライン映像情報の復号が終了するまで、前記ライン復号手段に対して、更新された前記フレーム鍵を用いて、次のライン音声情報及び次のライン映像情報を復号するように制御し、前記鍵更新手段に対して、更新された前記フレーム鍵を再度更新するように制御する繰返制御手段とを含むことを特徴とする請求項１６に記載の映像表示装置。
【請求項１８】　前記フレーム復号手段は、前記デジタル音声情報及び前記デジタル映像情報の復号において、同一の復号方式を用いることを特徴とする請求項１６に記載の映像表示装置。
【請求項１９】　前記ライン復号手段は、音声用初期値を設定し、設定した前記音声用初期値を用いて、ライン音声情報を復号し、次に、前記音声用初期値と同じ値を有する映像用初期値を設定し、設定した前記映像用初期値を用いて、ライン映像情報を復号することを特徴とする請求項１８に記載の映像表示装置。
【請求項２０】　前記復号手段は、前記映像表示装置による認証、前記フレーム鍵の生成及び暗号化された前記フレーム情報の復号において、共通の演算モジュールを用いることを特徴とする請求項１６に記載の映像表示装置。
【請求項２１】　前記送信手段は、さらに、前記デジタル映像情報の送信を示す前記映像イネーブル信号及び前記デジタル音声情報の送信を示す前記音声イネーブル信号を受信し、
前記抽出手段は、さらに、前記フレーム情報内で、前記映像イネーブル信号が示す期間において前記デジタル映像情報を抽出し、前記音声イネーブル信号が示す期間において前記デジタル音声情報を抽出することを特徴とする請求項１５に記載の映像表示装置。
【請求項２２】　前記受信手段は、前記デジタル音声情報及び前記デジタル映像情報の送信を識別する多重制御信号を受信し、
前記抽出手段は、前記多重制御信号を用いて、前記デジタル音声情報及び前記デジタル映像情報を抽出することを特徴とする請求項１４に記載の映像表示装置。
【請求項２３】　前記受信手段は、前記デジタル音声情報と前記デジタル映像情報との間に無信号期間を置いて、暗号化されたフレーム情報を受信し、
前記抽出手段は、前記デジタル音声情報と前記デジタル映像情報との間の無信号期間において、前記デジタル音声情報及び前記デジタル映像情報の受信を識別する多重制御信号を生成し、生成した前記多重制御信号を用いて、前記デジタル音声情報及び前記デジタル映像情報を抽出することを特徴とする請求項１４に記載の映像表示装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタルの映像信号及び音声信号を暗号化して伝送する暗号伝送システムに関する。
【０００２】
【従来の技術】ＬＣＤ（Liquid Crystal Display Device）やＣＲＴ（Cathode Ray Tube）へアナログの映像信号を伝送すると、波形のひずみなどにより表示画面ににじみやゴーストが発生する。
（ＤＶＩ規格）上記の問題を解決するために、ＤＶＩ（Digital Visual Interface）規格では、ＬＣＤやＣＲＴへのビデオ信号をデジタルにより伝送する。これにより、伝送ひずみの無い高品質の画面が表示できる。
【０００３】ＤＶＩ規格が適用された従来の信号伝送システムは、送信装置及び受信装置から構成され、送信装置及び受信装置は、伝送路を介して接続されている。送信装置は、３個のＴＭＤＳエンコーダ／シリアライザを備え、受信装置は、３個のＴＭＤＳデコーダ／リカバリーを備える。ＲＥＤ、ＧＲＥＥＮ、ＢＬＵＥからなる３個のコンポーネント信号は、それぞれ対応するＴＭＤＳ

エンコーダ／シリアライザに入力され、各ＴＭＤＳエンコーダ／シリアライザは、各コンポーネント信号をＴＭＤＳエンコードし、シリアライズして伝送路に送出する。次に、受信装置の各ＴＭＤＳデコーダ／リカバリーは、受信した信号をＴＭＤＳデコードし、リカバーしてコンポーネント信号を復元する。

【０００４】ＤＥ（データイネーブル）信号は、ＲＥＤ、ＧＲＥＥＮ、ＢＬＵＥなどのコンポーネント信号が存在する期間を示す信号であり、ＨＩＧＨアクティブである。例えば、ＤＥ信号がＬＯＷとなる期間は、映像の水平同期信号期間あるいは垂直同期信号期間である。ＣＴＬ信号には、ＣＴＬ０、ＣＴＬ１、ＣＴＬ２、ＣＴＬ３が制御信号として用意されている。なお、現在のＤＶＩ規格ではこれらの信号は未使用状態である。具体的には信号のレベルが常時０になっている。

【０００５】送信装置のＴＭＤＳエンコーダ／シリアライザは、８ビットで入力された映像信号を１０ビットに変換し、１０ビットに変換された映像信号をシリアライズして伝送路に送出する。８ビットから１０ビットへ変換する目的は、データの変化点を少なくして高速伝送に適した形にすることである。また、ＴＭＤＳエンコーダ／シリアライザは、コントロール信号２ビットを１０ビットに変換して伝送路に送出する。またデータイネーブル信号も合わせてエンコード、シリアライズされ伝送路に送出される。受信装置のＴＭＤＳデコーダ／リカバリーは、伝送路から受け取った１０ビットのシリアルデータを色信号の８ビット、データイネーブル信号、コントロール信号のそれぞれ２ビットにデコードして展開する。

【０００６】（ＨＤＣＰ規格）また、ＤＶＩ規格に適合した、デジタルコンテンツ保護システムとして、ＨＤＣＰ（High-bandwidth Digital Content Protection System）規格が提案されている。ＨＤＣＰ規格は、ＤＶＩ規格に適合する信号伝送システムを用いて、著作権保護が必要となる映像コンテンツを伝送するための規格であり、基本的には、送信装置と受信装置と間の認証、鍵共有、及び通信路上の映像コンテンツの暗号化からなる。

【０００７】ＨＤＣＰ規格を適用した信号伝送システムは、送信装置において、受信装置との認証及び鍵共有を行う認証部、共有した鍵を用いて映像情報を暗号化する暗号部、及びＴＭＤＳ符号化部を有し、受信装置において、送信装置との認証及び鍵共有を行う認証部、ＴＭＤＳ復号部、及び受信した信号を共有した鍵を用いて復号する復号部を有している。

【０００８】この構成により、送信装置と受信装置との間でI^2Cバスを介して、認証と鍵共有とをした後、送信装置は、映像ＲＧＢデータを暗号化して、ＤＶＩ規格のＴＭＤＳエンコーダを介して送信する。受信装置は、ＤＶＩ規格のＴＭＤＳ復号部を介して受信した後、送信装置と同じ鍵を用いて暗号化された映像ＲＧＢデータを復号し、もとの映像ＲＧＢデータを得る。ＨＤＣＰ規格では、ここで用いている暗号をＨＤＣＰ　Ｃｉｐｈｅｒと称しており、ＨＤＣＰ　Ｃｉｐｈｅｒのコアの部分は認証、鍵共有、及び映像データの暗号化において共通である。

【０００９】以上説明したように、ＤＶＩ規格及びＨＤＣＰ規格を適用するデータ伝送システムでは、伝送路上における映像の著作物としての保護をしながら、高品質の画像を伝送することができる。

【００１０】

【発明が解決しようとする課題】近年では、パーソナルコンピュータ、デジタル放送受信装置、ＤＶＤ再生装置などにおいて、デジタル音声の付加されたデジタル映像の再生が普及しており、映像に加えて音声についても、上記と同様に、高品質の伝送を行うことが要望されるようになってきている。

【００１１】そこで本発明はかかる要望に対処するために、映像情報と音声情報とを高品質で伝送することができる伝送システム、送信装置、受信装置、映像表示装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】上記目的を達成するために、本発明は、デジタル映像情報を帰線期間を置いて送信する送信装置と、前記デジタル映像情報を受信する受信装置とから構成される伝送システムであって、前記送信装置は、前記帰線期間においてデジタル音声情報を送信し、前記受信装置は、前記帰線期間において前記デジタル音声情報を受信することを特徴とする。

【００１３】また、本発明は、帰線期間を置いてデジタル映像情報を含むフレーム情報を生成し、暗号化して送信する送信装置と、暗号化された前記フレーム情報を受信して復号し、復号されたフレーム情報から前記デジタル映像情報を抽出し、表示する映像表示装置とから構成される暗号伝送システムであって、前記送信装置は、デジタル音声情報を前記帰線期間において前記フレーム情報に多重化し、前記デジタル音声情報が多重化されたフレーム情報を暗号化して送信し、前記映像表示装置は、暗号化された前記フレーム情報を受信し、復号してフレーム情報を生成し、生成した前記フレーム情報内に置かれた前記帰線期間から前記デジタル音声情報を抽出し、音声信号に変換することを特徴とする。

【００１４】また、本発明は、１以上の帰線期間を置いてデジタル映像情報を含むフレーム情報を生成し、暗号化して送信する送信装置であって、デジタル音声情報を前記帰線期間において前記フレーム情報に多重化する多重化手段と、前記デジタル音声情報が多重化された前記フレーム情報を暗号化する暗号化手段と、暗号化された前記フレーム情報を送信する送信手段とを備えることを特徴とする。

【００１５】ここで、生成された前記フレーム情報は、

垂直帰線期間を置き、続いて、ライン毎に水平帰線期間を置いてライン映像情報を含み、前記デジタル音声情報は、複数個のライン音声情報から構成され、前記多重化手段は、前記垂直帰線期間及び／又は前記水平帰線期間において前記ライン音声情報を多重化するように構成してもよい。

【００１６】ここで、前記暗号化手段は、フレーム情報に対応して、暗号化の鍵として用いられるフレーム鍵を生成するフレーム鍵生成手段と、フレーム情報に対応して生成された前記フレーム鍵を用いて、前記フレーム情報に含まれるデジタル音声情報及びデジタル映像情報を暗号化するフレーム暗号手段とを含むように構成してもよい。

【００１７】ここで、前記フレーム暗号手段は、前記フレーム鍵を用いて、前記フレーム情報に含まれるライン音声情報及びライン映像情報を暗号化するライン暗号手段と、前記フレーム鍵を更新する鍵更新手段と、前記フレーム情報に含まれる全てのライン音声情報及びライン映像情報の暗号化が終了するまで、前記ライン暗号化手段に対して、更新された前記フレーム鍵を用いて、次のライン音声情報及び次のライン映像情報を暗号化するように制御し、前記鍵更新手段に対して、更新された前記フレーム鍵を再度更新するように制御する繰返制御手段とを含むように構成してもよい。

【００１８】ここで、前記フレーム暗号手段は、前記デジタル音声情報及び前記デジタル映像情報の暗号化において、同一の暗号化方式を用いるように構成してもよい。ここで、前記ライン暗号手段は、音声用初期値を設定し、設定した前記音声用初期値を用いて、ライン音声情報を暗号化し、次に、前記音声用初期値と同じ値を有する映像用初期値を設定し、設定した前記映像用初期値を用いて、ライン映像情報を暗号化するように構成してもよい。

【００１９】ここで、前記送信装置は、暗号化された前記フレーム情報を映像表示装置に対して送信し、前記暗号化手段は、前記映像表示装置の認証、前記フレーム鍵の生成及び前記フレーム情報の暗号化において、共通の演算モジュールを用いるように構成してもよい。ここで、前記多重化手段は、さらに、前記フレーム情報内で前記デジタル映像情報を含む期間において、前記デジタル映像情報の送信を示す映像イネーブル信号を生成し、前記帰線期間において、前記デジタル音声情報の送信を示す音声イネーブル信号を生成し、前記送信手段は、さらに、生成された前記映像イネーブル信号及び前記音声イネーブル信号を送信するように構成してもよい。

【００２０】ここで、前記多重化手段は、前記デジタル音声情報を多重化する前記垂直帰線期間及び／又は前記水平帰線期間において、前記デジタル音声情報の送信を示す音声イネーブル信号を生成するように構成してもよい。ここで、前記多重化手段は、前記デジタル音声情報及び前記デジタル映像情報の送信を識別する多重制御信号を用いて、前記フレーム情報を生成し、前記送信手段は、前記多重制御信号を送信するように構成してもよい。

【００２１】ここで、前記多重化手段は、前記デジタル音声情報と前記デジタル映像情報との間に無信号期間を置いてフレーム情報を生成するように構成してもよい。

また、本発明は、前記送信装置から暗号化された前記フレーム情報を受信して復号し、復号されたフレーム情報から前記デジタル映像情報を抽出し、表示する映像表示装置であって、暗号化された前記フレーム情報を受信する受信手段と、暗号化された前記フレーム情報を復号する復号手段と、復号された前記フレーム情報内に置かれた前記帰線期間からデジタル音声情報を抽出し、他の期間からデジタル映像情報を抽出する抽出手段と、抽出した前記デジタル映像情報を表示し、抽出した前記デジタル音声情報を音声信号に変換する出力手段とを備えることを特徴とする。

【００２２】ここで、前記デジタル音声情報は、複数個のライン音声情報から構成されており、前記フレーム情報は、垂直帰線期間を置き、続いて、ライン毎に、水平帰線期間を置いてライン映像情報を含み、前記垂直帰線期間及び／又は前記水平帰線期間において、前記ライン音声情報が多重化されており、前記抽出手段は、前記垂直帰線期間及び／又は前記水平帰線期間から前記ライン音声情報を抽出するように構成してもよい。

【００２３】ここで、前記復号手段は、フレーム情報に対応して、復号の鍵として用いられるフレーム鍵を生成するフレーム鍵生成手段と、フレーム情報に対応して生成された前記フレーム鍵を用いて、暗号化された前記フレーム情報に含まれるデジタル音声情報及びデジタル映像情報を復号するフレーム復号手段とを含むように構成してもよい。

【００２４】ここで、前記フレーム復号手段は、前記フレーム鍵を用いて、暗号化された前記フレーム情報に含まれるライン音声情報及びライン映像情報を復号するライン復号手段と、前記フレーム鍵を更新する鍵更新手段と、暗号化された前記フレーム情報に含まれる全てのライン音声情報及びライン映像情報の復号が終了するまで、前記ライン復号手段に対して、更新された前記フレーム鍵を用いて、次のライン音声情報及び次のライン映像情報を復号するように制御し、前記鍵更新手段に対して、更新された前記フレーム鍵を再度更新するように制御する繰返制御手段とを含むように構成してもよい。

【００２５】ここで、前記フレーム復号手段は、前記デジタル音声情報及び前記デジタル映像情報の復号において、同一の復号方式を用いるように構成してもよい。ここで、前記ライン復号手段は、音声用初期値を設定し、設定した前記音声用初期値を用いて、ライン音声情報を復号し、次に、前記音声用初期値と同じ値を有する映像

用初期値を設定し、設定した前記映像用初期値を用いて、ライン映像情報を復号するように構成してもよい。

【００２６】ここで、前記復号手段は、前記映像表示装置による認証、前記フレーム鍵の生成及び暗号化された前記フレーム情報の復号において、共通の演算モジュールを用いるように構成してもよい。ここで、前記送信手段は、さらに、前記デジタル映像情報の送信を示す前記映像イネーブル信号及び前記デジタル音声情報の送信を示す前記音声イネーブル信号を受信し、前記抽出手段は、さらに、前記フレーム情報内で、前記映像イネーブル信号が示す期間において前記デジタル映像情報を抽出し、前記音声イネーブル信号が示す期間において前記デジタル音声情報を抽出するように構成してもよい。

【００２７】ここで、前記受信手段は、前記デジタル音声情報及び前記デジタル映像情報の送信を識別する多重制御信号を受信し、前記抽出手段は、前記多重制御信号を用いて、前記デジタル音声情報及び前記デジタル映像情報を抽出するように構成してもよい。ここで、前記受信手段は、前記デジタル音声情報と前記デジタル映像情報との間に無信号期間を置いて、暗号化されたフレーム情報を受信し、前記抽出手段は、前記デジタル音声情報と前記デジタル映像情報との間の無信号期間において、前記デジタル音声情報及び前記デジタル映像情報の受信を識別する多重制御信号を生成し、生成した前記多重制御信号を用いて、前記デジタル音声情報及び前記デジタル映像情報を抽出するように構成してもよい。

【００２８】

【発明の実施の形態】本発明に係る１の実施の形態としてのパーソナルコンピュータシステム１０について説明する。

１．パーソナルコンピュータシステム１０の構成

パーソナルコンピュータシステム１０は、図１に示すように、ＰＣ（パーソナルコンピュータ）本体装置２０、ＣＲＴディスプレイ装置３０、キーボード４１及びマウス４２から構成されている。ＰＣ本体装置２０とＣＲＴディスプレイ装置３０とは、ケーブル５０ａ及び５０ｂにより接続されている。

【００２９】また、ＰＣ本体装置２０は、図２に示すように、ビデオ接続部２０１、映像音声処理部２０２、ＤＶＤ入出力部２０３、制御部２０４及びその他の図示していないユニットから構成されている。また、ＰＣ本体装置２０は、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどを含み、前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、ＰＣ本体装置２０は、その機能を達成する。

【００３０】ＣＲＴディスプレイ装置３０は、ビデオ接続部３０１、ディスプレイ制御部３０２、ＣＲＴ部３０３、スピーカ制御部３０４及びスピーカ３０５を含んで構成されている。ビデオ接続部２０１は、図３に示すように、多重部２１１、ＨＤＣＰ暗号部２１５及びＴＭＤＳ符号化部２１３から構成される。ＨＤＣＰ暗号部２１５は、暗号部２１２及び認証鍵共有部２１４を含む。また、ビデオ接続部３０１は、図３に示すように、ＴＭＤＳ復号部３１１、ＨＤＣＰ復号部３１５及び分離部３１３から構成される。ＨＤＣＰ復号部３１５は、暗号部３１２及び認証鍵共有部３１４を含む。

【００３１】ＤＶＤは、映像情報が圧縮符号化された符号化映像情報と、音声情報が圧縮符号化された符号化音声情報とから構成される符号化映像音声情報を記録している。前記映像音声情報の一例は、動画像と音声情報とから構成される映画情報である。前記ＤＶＤは、利用者によりＤＶＤ入出力部２０３に装着される。ＰＣ本体装置２０は、ＰＣ本体装置２０に装着されたＤＶＤから、符号化映像音声情報を読み出し、読み出した符号化映像音声情報を分離して、符号化映像情報と符号化音声情報とを生成する。次に、符号化映像情報を復号して復号映像情報を生成する。ここで、復号映像情報と符号化音声情報とは、デジタル信号である。次に、ＰＣ本体装置２０は、復号映像情報と符号化音声情報とをそれぞれ暗号化して暗号化映像情報と暗号化音声情報とを生成し、生成した暗号化映像情報と暗号化音声情報とをケーブル５０ａを介して、ＣＲＴディスプレイ装置３０へ出力する。ＣＲＴディスプレイ装置３０は、暗号化映像情報と暗号化音声情報とを受け取り、受け取った暗号化映像情報と暗号化音声情報とを復号して、復号映像情報と復号音声情報とを生成し、生成した復号映像情報をＣＲＴ部３０３に表示し、生成した復号音声情報をアナログの音声信号に変換してスピーカ３０５により出力する。

【００３２】１．１　キーボード４１、マウス４２、制御部２０４、ＤＶＤ入出力部２０３及び映像音声処理部２０２

キーボード４１及びマウス４２は、利用者から、前記ＤＶＤに記録されている前記符号化映像音声情報を再生する指示の入力を受け付け、入力を受け付けた指示に対応する指示情報を生成し、生成した指示情報を制御部２０４へ出力する。

【００３３】制御部２０４は、前記指示情報を受け取り、受け取った指示情報に基づいて、前記符号化映像音声情報の読出指示をＤＶＤ入出力部２０３へ出力する。ＤＶＤ入出力部２０３は、前記読出指示を受け取り、受け取った読出指示に基づいて、前記ＤＶＤから前記符号化映像音声情報を読み出し、読み出した前記符号化映像音声情報を映像音声処理部２０２へ出力する。

【００３４】映像音声処理部２０２は、前記符号化映像音声情報を受け取り、受け取った前記符号化映像音声情報を分離して、符号化映像情報と符号化音声情報とを生成し、生成した符号化映像情報を復号して復号映像情報を生成し、生成した復号映像情報と生成した符号化音声

情報とをビデオ接続部２０１へ出力する。

１．２　ビデオ接続部２０１

（１）多重部２１１

多重部２１１は、映像音声処理部２０２から復号映像情報と符号化音声情報とを受け取る。

【００３５】復号映像情報は、１フレームに相当するフレーム映像情報を複数個含む。前記複数のフレーム映像情報が連続して表示されることにより、ＣＲＴディスプレィ装置３０において、動画像が表現される。また、各フレーム映像情報は、１ラインに相当するライン映像情報を４８０個含む。また、符号化音声情報は、前記フレーム映像情報に対応するフレーム音声情報を含む。フレーム音声情報は、対応するフレーム映像情報がＣＲＴディスプレィ装置３０において、再生される時間帯内において、音声に変換されて出力される。また、各フレーム音声情報は、前記ライン映像情報に対応するライン音声情報を４８０個含む。

【００３６】多重部２１１は、前記復号映像情報のうち、１個のフレーム映像情報をＰＣ本体装置２０からＣＲＴディスプレィ装置３０へ伝送する際に、ＰＣ本体装置２０とＣＲＴディスプレィ装置３０との間において、前記フレーム映像情報を表示するための同期を確立するために、前記フレーム映像情報が伝送される直前において、所定数個の垂直同期信号が送信される時刻を含む垂直帰線期間を設ける。次に、１個のフレーム映像情報内の各ライン映像情報を表示するための同期を確立するために、各ライン映像情報が伝送される直前において、水平同期信号が送信される時刻を含む水平帰線期間を設ける。

【００３７】垂直帰線期間、水平帰線期間及び１個のフレーム映像情報の関係を図４に示す。この図に示すように、各フレーム映像情報は、４８０個のライン映像情報から構成され、各ライン映像情報は、７２０画素から構成されるものとしている。また、各画素は、２４ビットからなり、各画素は、ＲＥＤ、ＧＲＥＥＮ、ＢＬＵＥ用のコンポーネント情報をそれぞれ８ビットずつ含む。この図に示すように、多重部２１１は、１個のフレーム映像情報を伝送する直前において、４５個のライン映像情報の伝送に相当する時間帯を垂直帰線期間として設ける。次に、各ライン映像情報を伝送する直前において、１３８個の画素の伝送に相当する時間帯を水平帰線期間として設ける。

【００３８】多重部２１１は、図５に示すように、受け取った復号映像情報のうち、１個のフレーム映像情報について、前記垂直帰線期間の開始時点において、映像信号用のデータイネーブル信号ＤＥをＬＯＷに設定し、音声信号用のデータイネーブル信号ＡＤＥをＬＯＷに設定し、ＬＯＷに設定されたデータイネーブル信号ＤＥ及びＡＤＥをＴＭＤＳ符号化部２１３へ出力する。

【００３９】次に、前記垂直帰線期間内において、後述するように、ＨＤＣＰ暗号部２１５がフレーム鍵の計算を完了した時、この時点から音声信号用のデータイネーブル信号ＡＤＥをＨＩＧＨに設定し、ＨＩＧＨに設定されたデータイネーブル信号ＡＤＥをＴＭＤＳ符号化部２１３へ出力する。また、この時点から符号化音声情報の出力を開始する。

【００４０】図５は、１個のフレーム映像情報が伝送される時間帯内におけるデータイネーブル信号ＤＥ、ＡＤＥ、復号映像情報、符号化音声情報の時間的変化を示している。この図において、時間は、ライン４０１の左端から右端に向かって経過する。続いて、ライン４０２の左端から右端に向かって経過する。以下、ライン４０３、４０４、・・・、４０５において同様である。

【００４１】ライン４０１、４０２、・・・、４０３が示す時間帯は、前記垂直帰線期間である。ライン４０１が示す時間帯において、多重部２１１は、データイネーブル信号ＤＥをＬＯＷに設定し、データイネーブル信号ＡＤＥをＬＯＷに設定する。また、この時間帯において、復号映像情報及び符号化音声情報を出力しない。また、ライン４０１が示す時間帯の開始時点において、ＨＤＣＰ暗号部２１５によるフレーム鍵の計算が開始される。

【００４２】ライン４０２が示す時間帯の開始時点において、上記と同様に、多重部２１１は、データイネーブル信号ＤＥ及びＡＤＥをＬＯＷに設定する。次に、ライン４０２が示す時間帯内において、上述したＨＤＣＰ暗号部２１５によるフレーム鍵の計算が完了したとすると、この完了時点から音声信号用のデータイネーブル信号ＡＤＥをＨＩＧＨに設定し、ＨＩＧＨに設定されたデータイネーブル信号ＡＤＥをＴＭＤＳ符号化部２１３へ出力する。また、この時点から１個の音声映像情報の出力を開始する。

【００４３】ライン４０２の次のラインからライン４０３までが示す時間帯において、多重部２１１は、データイネーブル信号ＤＥをＬＯＷに設定し、音声信号用のデータイネーブル信号ＡＤＥをＨＩＧＨに設定し、データイネーブル信号ＤＥ及びＡＤＥをＴＭＤＳ符号化部２１３へ出力する。また、多重部２１１は、継続して前記１個のライン映像情報の出力し続けている。

【００４４】次に、ライン４０４が示す時間帯において、水平帰線期間に相当する時間帯内で、多重部２１１は、データイネーブル信号ＤＥをＬＯＷに設定し、ＬＯＷに設定されたデータイネーブル信号ＤＥをＴＭＤＳ符号化部２１３へ出力する。次に、水平帰線期間の終了直後から始まる１個のライン映像情報の期間については、多重部２１１は、データイネーブル信号ＤＥをＨＩＧＨに設定し、ＨＩＧＨに設定されたデータイネーブル信号ＤＥをＴＭＤＳ符号化部２１３へ出力する。

【００４５】また、ライン４０４が示す時間帯において、多重部２１１は、水平帰線期間において、音声信号

用のデータイネーブル信号ＡＤＥをＨＩＧＨに設定して出力し、前記１個のライン音声情報を継続して暗号部２１２へ出力する。ここで、ライン４０２～ライン４０４において継続して出力される１個のライン音声情報は、ＨＤＣＰ暗号部２１５がフレーム鍵の計算を完了した時点により定まる個数の音声セルから構成される。各音声セルは、２４ビット長の符号化音声情報から構成される。また、多重部２１１は、水平帰線期間の終了直後から始まる１個のライン映像情報の期間において、１個のライン映像情報を暗号部２１２へ出力する。１個のライン映像情報は、７２０画素からなる。

【００４６】図６に、ライン４０４の次のラインからライン４０５までが示す各時間帯内におけるデータイネーブル信号ＤＥ、ＡＤＥ、符号化音声情報、及び復号映像情報の関係を示す。この図に示すように、多重部２１１は、水平帰線期間において、１個のライン音声情報を暗号部２１２へ出力する。ここで、１個のライン音声情報は、１３８個の音声セルから構成される。各音声セルは、２４ビット長の符号化音声情報から構成される。また、多重部２１１は、水平帰線期間の終了直後から始まる１個のライン映像情報の期間において、１個のライン映像情報を暗号部２１２へ出力する。１個のライン映像情報は、７２０画素からなる。

【００４７】また、多重部２１１は、垂直帰線期間内において、前記所定数個の垂直同期信号ＶＳＹＮＣを生成し、生成した前記垂直同期信号ＶＳＹＮＣをＴＭＤＳ符号化部２１３へ出力する。また、水平帰線期間内において、水平同期信号ＨＳＹＮＣを生成し、生成した水平同期信号ＨＳＹＮＣをＴＭＤＳ符号化部２１３へ出力する。

【００４８】（２）認証鍵共有部２１４

認証鍵共有部２１４は、ＨＤＣＰ規格に従って動作する。認証鍵共有部２１４の主要な動作は、認証鍵共有部２１４と受信側の装置との間の機器認証、鍵共有、暗号化のための乱数の生成などである。認証鍵共有部２１４の詳細については、ＨＤＣＰ規格に規定されているので説明を省略する。

【００４９】認証鍵共有部２１４は、I^2Cバスであるケーブル５０ｂを介して、後述する認証鍵共有部３１４と接続されている。なお、本実施の形態における認証鍵共有部２１４の特有の機能及び構成などについては、後述する。

（３）暗号部２１２

暗号部２１２は、動作クロック毎に、多重部２１１から画素及び音声セルを受け取り、認証鍵共有部２１４から乱数ＰＲｊを受け取る。

【００５０】次に、画素を受け取った場合に、暗号部２１２は、式１に示すように、受け取った画素と乱数ＰＲｊとに排他的論理和をビット毎に施して、暗号化画素を生成し、生成した暗号化画素をＴＭＤＳ符号化部２１３へ出力する。

（式１）暗号化画素＝画素（＋）乱数ＰＲｊ

ここで、演算子（＋）は、排他的論理和を示す。

【００５１】また、音声セルを受け取った場合に、同様に、暗号部２１２は、式２に示すように、受け取った音声セルと乱数ＰＲｊとに排他的論理和をビット毎に施して、暗号化音声セルを生成し、生成した暗号化音声セルをＴＭＤＳ符号化部２１３へ出力する。

（式２）暗号化音声セル＝音声セル（＋）乱数ＰＲｊ

（４）ＴＭＤＳ符号化部２１３

ＴＭＤＳ符号化部２１３は、ケーブル５０ａを介して、後述するＴＭＤＳ復号部３１１と接続されている。

【００５２】ＴＭＤＳ符号化部２１３は、図７に示すように、ＴＭＤＳエンコーダ・シリアライザ２１３ａ、２１３ｂ及び２１３ｃから構成されている。ＴＭＤＳエンコーダ・シリアライザ２１３ａ、２１３ｂ及び２１３ｃは、この図に示すように、それぞれ、ケーブル５０ａ内のチャネルＣ１２、Ｃ１１及びＣ１０を介して、後述するＴＭＤＳデコーダ・リカバリ３１１ａ、３１１ｂ及び３１１ｃと接続されている。

【００５３】（ＴＭＤＳエンコーダ・シリアライザ２１３ａ）ＴＭＤＳエンコーダ・シリアライザ２１３ａは、暗号部２１２から暗号化画素のうちのＲＥＤのコンポーネント情報、及び音声セルの先頭８ビットを受け取る。また、多重部２１１から映像信号用のデータイネーブル信号ＤＥ、音声信号用のデータイネーブル信号ＡＤＥ及びその他の制御信号を受け取る。

【００５４】ＴＭＤＳエンコーダ・シリアライザ２１３ａは、受け取った８ビットのＲＥＤのコンポーネント情報及び音声セルの先頭８ビット［２３：１６］、データイネーブル信号ＤＥ、データイネーブル信号ＡＤＥ及びその他の制御信号をＴＭＤＳエンコードし、シリアライズしてチャネルＣ１２を介して、ＴＭＤＳデコーダ・リカバリ３１１ａへ送出する。

【００５５】具体的には、ＴＭＤＳエンコーダ・シリアライザ２１３ａは、８ビットのＲＥＤのコンポーネント情報及び音声セルの先頭８ビット［２３：１６］をそれぞれ１０ビットの情報に変換し、１０ビットの情報をシリアライズして送出する。８ビットから１０ビットへ変換するのは、この変換によりデータの変化点を少なくして高速伝送に適した形にするためである。また、ＴＭＤＳエンコーダ・シリアライザ２１３ａは、２ビットのコントロール信号であるデータイネーブル信号ＤＥ、ＡＤＥを１０ビットに変換して送出する。

【００５６】（ＴＭＤＳエンコーダ・シリアライザ２１３ｂ）ＴＭＤＳエンコーダ・シリアライザ２１３ｂは、暗号部２１２から暗号化画素のうちのＧＲＥＥＮのコンポーネント情報及び音声セルの中央８ビット［１５：８］を受け取る。また、多重部２１１から映像信号用のデータイネーブル信号ＤＥ及びその他の制御信号を受け

取る。

【００５７】ＴＭＤＳエンコーダ・シリアライザ２１３ｂは、受け取ったＧＲＥＥＮのコンポーネント情報、音声セルの中央８ビット［１５：８］、データイネーブル信号ＤＥ及びその他の制御信号を、上記と同様に、ＴＭＤＳエンコードし、シリアライズしてチャネルＣ１１を介して、ＴＭＤＳデコーダ・リカバリ３１１ｂへ送出する。

【００５８】（ＴＭＤＳエンコーダ・シリアライザ２１３ｃ）ＴＭＤＳエンコーダ・シリアライザ２１３ｃは、暗号部２１２から暗号化画素のうちのＢＬＵＥのコンポーネント情報及び音声セルの末尾８ビット［０：７］を受け取る。また、多重部２１１から映像信号用のデータイネーブル信号ＤＥ、垂直同期信号ＶＳＹＮＣ及び水平同期信号ＨＳＹＮＣを受け取る。

【００５９】ＴＭＤＳエンコーダ・シリアライザ２１３ｃは、受け取ったＢＬＵＥのコンポーネント情報、音声セルの末尾８ビット［０：７］、データイネーブル信号ＤＥ、垂直同期信号ＶＳＹＮＣ及び水平同期信号ＨＳＹＮＣを、上記と同様に、ＴＭＤＳエンコードし、シリアライズしてチャネルＣ１０を介して、ＴＭＤＳデコーダ・リカバリ３１１ｃへ送出する。

【００６０】１．３　ビデオ接続部３０１

（１）ＴＭＤＳ復号部３１１

ＴＭＤＳ復号部３１１は、図７に示すように、ＴＭＤＳデコーダ・リカバリ３１１ａ、３１１ｂ及び３１１ｃから構成されている。

（ＴＭＤＳデコーダ・リカバリ３１１ａ）ＴＭＤＳデコーダ・リカバリ３１１ａは、チャネルＣ１２を介して、ＴＭＤＳ符号化部２１３からシリアルデータを受け取り、受け取ったシリアルデータから８ビットのＲＥＤのコンポーネント情報、音声セルの先頭８ビット［２３：１６］、データイネーブル信号ＤＥ、データイネーブル信号ＡＤＥ及びその他の制御信号を復号し、ＲＥＤのコンポーネント情報及び音声セルの先頭８ビット［２３：１６］を暗号部３１２へ出力し、データイネーブル信号ＤＥ、データイネーブル信号ＡＤＥ及びその他の制御信号ををを分離部３１３へ出力する。

【００６１】（ＴＭＤＳデコーダ・リカバリ３１１ｂ）ＴＭＤＳデコーダ・リカバリ３１１ｂは、チャネルＣ１１を介して、ＴＭＤＳ符号化部２１３からシリアルデータを受け取り、受け取ったシリアルデータからＧＲＥＥＮのコンポーネント情報及び音声セルの中央８ビット［１５：８］を復号し、ＧＲＥＥＮのコンポーネント情報及び音声セルの中央８ビット［１５：８］を暗号部３１２へ出力する。

【００６２】（ＴＭＤＳデコーダ・リカバリ３１１ｃ）ＴＭＤＳデコーダ・リカバリ３１１ｃは、チャネルＣ１０を介して、ＴＭＤＳ符号化部２１３からシリアルデータを受け取り、受け取ったシリアルデータからＢＬＵＥのコンポーネント情報、音声セルの末尾８ビット［７：０］、垂直同期信号ＶＳＹＮＣ及び水平同期信号ＨＳＹＮＣを復号し、ＢＬＵＥのコンポーネント情報、音声セルの末尾８ビット［７：０］を暗号部３１２へ出力し、垂直同期信号ＶＳＹＮＣ及び水平同期信号ＨＳＹＮＣをディスプレィ制御部３０２へ出力する。

【００６３】（２）認証鍵共有部３１４

認証鍵共有部３１４は、認証鍵共有部２１４と同様に、ＨＤＣＰ規格に従って動作する。認証鍵共有部３１４の主要な動作は、認証鍵共有部３１４と送信側の装置との間の機器認証、鍵共有、暗号化のための乱数の生成などである。認証鍵共有部３１４の詳細については、ＨＤＣＰ規格に規定されているので説明を省略する。

【００６４】なお、本実施の形態における認証鍵共有部３１４の特有の機能及び構成などについては、後述する。

（３）暗号部３１２

暗号部３１２は、暗号部２１２と同様に動作する。暗号部３１２は、動作クロック毎に、ＴＭＤＳ復号部３１１から暗号化画素及び暗号化音声セルを受け取り、認証鍵共有部３１４から乱数ＰＲｊを受け取る。

【００６５】次に、暗号化画素を受け取った場合に、暗号部３１２は、式３に示すように、受け取った暗号化画素と乱数ＰＲｊとに排他的論理和をビット毎に施して、復号画素を生成し、生成した復号画素を分離部３１３へ出力する。

（式３）復号画素＝暗号化画素（＋）乱数ＰＲｊ

ここで、式１において、暗号化画素が生成される際に用いられた乱数と、式３において、復号画素が生成される際に用いられた乱数とは、同一の値を有するので、元の画素が復号される。

【００６６】また、暗号化音声セルを受け取った場合に、同様に、暗号部３１２は、式４に示すように、受け取った暗号化音声セルと乱数ＰＲｊとに排他的論理和をビット毎に施して、復号音声セルを生成し、生成した復号音声セルを分離部３１３へ出力する。

（式４）復号音声セル＝暗号化音声セル（＋）乱数ＰＲｊ

ここで、式２において、暗号化音声セルが生成される際に用いられた乱数と、式４において、復号音声セルが生成される際に用いられた乱数とは、同一の値を有するので、元の音声セルが復号される。

【００６７】（４）分離部３１３

分離部３１３は、動作クロック毎に、暗号部３１２から２４ビット長の情報を受け取り、ＴＭＤＳ復号部３１１からデータイネーブル信号ＤＥ及びデータイネーブル信号ＡＤＥを受け取る。分離部３１３は、受け取ったデータイネーブル信号ＤＥがＨＩＧＨの場合、受け取った２４ビット長の情報が復号画素であるとみなし、動作クロック毎に、受け取った２４ビット長の情報を復号画素と

して、ディスプレィ制御部３０２へ出力する。また、分離部３１３は、受け取ったデータイネーブル信号ＤＥをディスプレィ制御部３０２へ出力する。

【００６８】また、分離部３１３は、受け取ったデータイネーブル信号ＡＤＥがＨＩＧＨの場合、受け取った２４ビット長の情報が復号音声セルであるとみなし、動作クロック毎に、受け取った２４ビット長の情報を復号音声セルとして、スピーカ制御部３０４へ出力する。また、分離部３１３は、受け取ったデータイネーブル信号ＡＤＥをスピーカ制御部３０４へ出力する。

【００６９】１．４　ディスプレィ制御部３０２及びＣＲＴ部３０３

ディスプレィ制御部３０２は、分離部３１３から動作クロック毎に、復号画素及びデータイネーブル信号ＤＥを受け取り、ＴＭＤＳ復号部３１１から垂直同期信号ＶＳＹＮＣ及び水平同期信号ＨＳＹＮＣを受け取る。ディスプレィ制御部３０２は、動作クロック毎に受け取った復号画素、データイネーブル信号ＤＥ、垂直同期信号ＶＳＹＮＣ及び水平同期信号ＨＳＹＮＣに基づいて、ＲＥＤ、ＧＲＥＥＮ及びＢＬＵＥのアナログ信号を生成し、生成した各アナログ信号をＣＲＴ部３０３へ出力する。

【００７０】ＣＲＴ部３０３は、ディスプレィ制御部３０２からＲＥＤ、ＧＲＥＥＮ及びＢＬＵＥのアナログ信号を受け取り、カラーの画像を表示する。

１．５　スピーカ制御部３０４及びスピーカ３０５

スピーカ制御部３０４は、分離部３１３から動作クロック毎に復号音声セル及びデータイネーブル信号ＡＤＥを受け取り、受け取ったデータイネーブル信号ＡＤＥがＨＩＧＨの間、受け取った復号音声セルを復号して音声情報を生成し、生成した音声情報を変換してアナログ信号を生成し、生成したアナログ信号をスピーカ３０５へ出力する。

【００７１】スピーカ３０５は、スピーカ制御部３０４からアナログ信号を受け取り、受け取ったアナログ信号を変換して音声を生成し、出力する。

２．パーソナルコンピュータシステム１０の動作

パーソナルコンピュータシステム１０の動作について説明する。

（１）パーソナルコンピュータシステム１０の概要動作

利用者の指示により、ＤＶＤに記録されている符号化映像音声情報を再生する場合のパーソナルコンピュータシステム１０の概要動作について、図８に示すフローチャートを用いて説明する。

【００７２】ＰＣ本体装置２０とＣＲＴディスプレィ装置３０との間において、ＨＤＣＰ規格に基づいて、ＰＣ本体装置２０は、ＣＲＴディスプレィ装置３０が正当な装置であるか否かを認証し（ステップＳ１０１）、認証が失敗した場合に（ステップＳ１０２）、処理を終了する。認証が成功した場合に（ステップＳ１０２）、ＨＤＣＰ規格に基づいてＫＳＶリストを生成する（ステップＳ１０３）。ここで、ＫＳＶリストの生成については、ＨＤＣＰ規格に記載されているので、説明を省略する。

【００７３】次に、フレームの番号を示す変数ｉに０の値を設定する（ステップＳ１０４）。次に、ステップＳ１０５からＳ１１２において、フレーム毎に、ステップＳ１０５からＳ１１１に示す処理を繰り返す。変数ｉに１の値を加算し（ステップＳ１０６）、フレーム毎の鍵共有を行う（ステップＳ１０７）。次に、ステップＳ１０８からＳ１１１において、ライン毎に、ステップＳ１０９からＳ１１０を繰り返す。

【００７４】１個のライン音声情報及び１個のライン映像情報の暗号化、送信及び復号を行い（ステップＳ１０９）、ＨＤＣＰ規格に基づいて、鍵の更新を行う（ステップＳ１１０）。

（２）装置認証の動作

図８のステップＳ１０１に示す装置認証の動作について、図９に示すフローチャートを用いて説明する。なお、装置認証については、ＨＤＣＰ規格に記載されているので、詳細な説明を省略する。

【００７５】認証鍵共有部２１４は、Ａｎを生成し（ステップＳ１７１）、Ａｎ及びＡｋｓｖをI^2Cバスであるケーブル５０ｂを介して認証鍵共有部３１４へ送信する（ステップＳ１７２）。認証鍵共有部３１４は、Ｂｋｓｖ及びＲＥＰＥＡＴＥＲをI^2Cバスであるケーブル５０ｂを介して認証鍵共有部２１４へ送信する（ステップＳ１７３）。

【００７６】認証鍵共有部２１４は、Ｋｍ＝Ａｋｅｙｓ　ｏｖｅｒ　Ｂｋｓｖを算出し（ステップＳ１７４）、（K_s、M_O、R_O）＝ｄｖｉＢｌｋＣｉｐｈｅｒ（Ｋｍ、ＲＥＰＥＡＴＥＲ｜｜Ａｎ）を算出する（ステップＳ１７５）。認証鍵共有部３１４は、Ｋｍ’＝Ｂｋｅｙｓ　ｏｖｅｒ　Ａｋｓｖを算出し（ステップＳ１７６）、（K_s’、M_O’、R_O’）＝ｄｖｉＢｌｋＣｉｐｈｅｒ（Ｋｍ’、ＲＥＰＥＡＴＥＲ｜｜Ａｎ）を算出し（ステップＳ１７７）、R_O’をI^2Cバスであるケーブル５０ｂを介して認証鍵共有部２１４へ送信する（ステップＳ１７８）。

【００７７】認証鍵共有部２１４は、R_OとR_O’とを比較し、一致する場合には（ステップＳ１７９）、ＣＲＴディスプレィ装置３０が正当な装置であると認証する。また、一致しない場合には（ステップＳ１７９）、ＣＲＴディスプレィ装置３０が正当な装置でないと認証する。（３）フレーム毎の鍵共有の動作図８のステップＳ１０７に示すフレーム毎の鍵共有の動作について、図１０に示すフローチャートを用いて説明する。なお、フレーム毎の鍵共有については、ＨＤＣＰ規格に記載されているので、詳細な説明を省略する。

【００７８】認証鍵共有部２１４は、（Ｋｉ、Ｍｉ、Ｒｉ）＝ｄｖｉＢｌｋＣｉｐｈｅｒ（Ｋｓ、ＲＥＰＥＡＴＥＲ｜｜M_{i-1}）を算出する（ステップＳ１３１）。次

に、認証鍵共有部２１４は、（ｉ　ｍｏｄ　１２８）が０である場合にのみ（ステップＳ１３２）、Ｒｉ＝ｒｉを算出する（ステップＳ１３３）。認証鍵共有部３１４は、（Ｋｉ’、Ｍｉ’、Ｒｉ’）＝ｄｖｉＢｌｋＣｉｐｈｅｒ（Ｋｓ’、ＲＥＰＥＡＴＥＲ｜｜M'_{i-1}）を算出する（ステップＳ１４１）。次に、認証鍵共有部３１４は、（ｉ　ｍｏｄ　１２８）が０である場合にのみ（ステップＳ１４２）、Ｒｉ’＝ｒｉ’を算出する（ステップＳ１４３）。次に、認証鍵共有部３１４は、２秒毎に、Ｒｉ’をＩ２Ｃバスであるケーブル５０ｂを介して認証鍵共有部２１４へ送信する認証鍵共有部２１４は、２秒毎に、ＲｉとＲｉ’とを比較し、一致する場合には（ステップＳ１３５）、ＣＲＴディスプレィ装置３０が正当な装置であると認証する。また、一致しない場合には（ステップＳ１３５）、ＣＲＴディスプレィ装置３０が正当な装置でないと認証する。

【００７９】（４）１個のライン音声情報及び１個のライン映像情報の暗号化、送信及び復号の動作

図８のステップＳ１０９に示す１個のライン音声情報及び１個のライン映像情報の暗号化、送信及び復号の動作について、図１１に示すフローチャートを用いて説明する。

【００８０】認証鍵共有部２１４は、ＨＤＣＰ規格において規定されている乱数生成の際に用いられる初期値を保存初期値として一旦記憶する。ここで、前記初期値は、具体的には、M_{i-1}である。（ステップＳ２００）。次に、ステップＳ２０１～ステップＳ２０５において、１個のライン音声情報内の各音声セルＡＣｊについて、以下のステップＳ２０２～Ｓ２０４を繰り返す。ここで、１個のライン音声情報内には、１３８個の音声セルが含まれる。変数ｊは、上記の繰り返しにおいて、１～１３８の値をとる。

【００８１】認証鍵共有部２１４は、２４ビットの乱数ＰＲｊを生成し（ステップＳ２０２）、暗号部２１２は、音声セルＡＣｊと乱数ＰＲｊに排他的論理和を施して暗号化音声セルＥＡＣｊを生成する（ステップＳ２０３）。次に、暗号部２１２は、ＴＭＤＳ符号化部２１３、ケーブル５０ａ、ＴＭＤＳ復号部３１１を介して、暗号部３１２へ、生成した暗号化音声セルＥＡＣｊを送信する（ステップＳ２０４）。

【００８２】認証鍵共有部３１４は、ＨＤＣＰ規格において規定されている乱数生成の際に用いられる初期値を保存初期値として一旦記憶する。ここで、前記初期値は、具体的には、M'_{i-1}である。（ステップＳ２２１）。次に、ステップＳ２２２～ステップＳ２２５において、１個のライン音声情報内の各暗号化音声セルＤＡＣｊについて、以下のステップＳ２２３、Ｓ２０４、Ｓ２２４を繰り返す。ここで、１個のライン音声情報内には、１３８個の暗号化音声セルが含まれる。変数ｊは、上記の繰り返しにおいて、１～１３８の値をとる。

【００８３】認証鍵共有部３１４は、２４ビットの乱数ＰＲｊを生成し（ステップＳ２２３）、暗号部３１２は、暗号化音声セルＤＡＣｊと乱数ＰＲｊに排他的論理和を施して復号音声セルＤＡＣｊを生成し、暗号部３１２は、分離部３１３へ生成した復号音声セルＤＡＣｊを出力する（ステップＳ２２４）。認証鍵共有部２１４は、前記一旦記憶した保存初期値から前記初期値を復元する（ステップＳ２０６）。次に、ステップＳ２０７～Ｓ２１１において、１個のライン映像情報内の各画素ＰＣｊについて、以下のステップＳ２０８～Ｓ２１０を繰り返す。ここで、１個のライン映像情報内には、７２０個の画素が含まれる。変数ｊは、上記の繰り返しにおいて、１～７２０の値をとる。

【００８４】認証鍵共有部２１４は、２４ビットの乱数ＰＲｊを生成し（ステップＳ２０８）、暗号部２１２は、画素ＰＣｊと生成した乱数ＰＲｊとに排他的論理和を施して暗号化画素ＥＰＣｊを生成し（ステップＳ２０９）、暗号部２１２は、ＴＭＤＳ符号化部２１３、ケーブル５０ａ、ＴＭＤＳ復号部３１１を介して、暗号部３１２へ、生成した暗号化画素ＥＰＣｊを送信する（ステップＳ２１０）。

【００８５】認証鍵共有部３１４は、前記一旦記憶した保存初期値から前記初期値を復元する（ステップＳ２２６）。次に、ステップＳ２２７～Ｓ２３０において、１個のライン映像情報内の各暗号化画素ＤＰＣｊについて、以下のステップＳ２２８、Ｓ２１０、Ｓ２２９を繰り返す。ここで、１個のライン映像情報内には、７２０個の暗号化画素が含まれる。変数ｊは、上記の繰り返しにおいて、１～７２０の値をとる。

【００８６】認証鍵共有部３１４は、２４ビットの乱数ＰＲｊを生成し（ステップＳ２２８）、暗号部３１２は、暗号化画素ＤＰＣｊと生成した乱数ＰＲｊとに排他的論理和を施して復号画素ＤＰＣｊを生成し、生成した復号画素ＤＰＣｊを分離部３１３へ出力する（ステップＳ２２９）。

（５）ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］による暗号化［復号］の状態遷移

ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］による暗号化［復号］の状態遷移について、図１２を用いて説明する。なお、ここでは、［　］内の記載は、ＨＤＣＰ復号部３１５による復号の状態遷移を示している。

【００８７】（何れかの状態からアイドル状態Ｄ０への遷移）Ｒｅｓｅｔ状態にある場合（ステップＳ３０１）、又は認証に失敗した場合に（ステップＳ３０４）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、アイドル状態Ｄ０に遷移する。

（アイドル状態Ｄ０からフレーム鍵計算状態Ｄ１への遷移）ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、ＨＤＣＰ規格に基づき、ＤＶＩ規格では未使用であったＣＴＬ３信号をフレーム鍵計算の同期信号に用い

る。認証が成功したときであって、ＤＶＩインターフェイスのＣＴＬ３信号を生成したときに（ステップＳ３０２）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、フレーム鍵計算を行なうフレーム鍵計算状態Ｄ１に遷移する。フレーム鍵計算状態Ｄ１において、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、次の映像フレームの暗号化［復号］のために用いるフレーム鍵を計算する。

【００８８】（フレーム鍵計算状態Ｄ１から映像暗号化［復号］状態Ｄ２への遷移）Ｖブランク期間中に、音声信号の開始信号がないとき、暗号化［復号］すべき映像信号の先頭を与えるＤＥ信号を受け取ると（ステップＳ３０９）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像暗号化［復号］状態Ｄ２に遷移する。映像暗号化［復号］状態Ｄ２において、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像信号を暗号化［復号］する。

【００８９】（映像暗号化［復号］状態Ｄ２からUnknown Blank状態Ｄ３への遷移）映像信号の終わり（一般に行の最後かフレームの最後）がＤＥにより通知される。図１２において、この信号を「！ＤＥ」と表現している。！ＤＥを受け取ると（ステップＳ３０８）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、Unknown Blank状態Ｄ３に遷移する。Unknown Blank状態Ｄ３において、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、鍵更新を始める。

【００９０】（Unknown Blank状態Ｄ３からフレーム鍵計算状態Ｄ１への遷移）Unknown Blank状態Ｄ３において、ＣＴＬ３信号を受け取ると（ステップＳ３０３）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、新たな映像フレーム鍵計算を行なうフレーム鍵計算状態Ｄ１へ遷移する。（Unknown Blank状態Ｄ３からＨブランク状態Ｄ４への遷移）ＨｓｙｎｃによりＨブランク（一般に行間）であることが分かる。Ｈｓｙｎｃを受け取ると（ステップＳ３１０）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、Ｈブランク状態Ｄ４へ遷移する。

【００９１】Ｈブランク状態Ｄ４において、鍵更新がＤ３でUnknown Blank状態完了しなければ、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、ここで待つ。（Unknown Blank状態Ｄ３からＶブランク状態Ｄ５への遷移）ＶｓｙｎｃによりＶブランク（一般にフレーム間）であることが分かる。Ｖｓｙｎｃを受け取ると（ステップＳ３１８）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、Ｖブランク状態Ｄ５へ遷移する。

【００９２】（Ｈブランク状態Ｄ４から映像暗号化［復号］状態Ｄ２への遷移）Ｈブランキング期間に音声信号がないとき、ＤＥ信号を受け取ると（ステップＳ３１４）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像信号の次の行の暗号化［復号］を始め、映像暗号化［復号］状態Ｄ２へ遷移する。

（Ｈブランク状態Ｄ４からフレーム鍵計算状態Ｄ１への遷移）ＣＴＬ３信号が発生すれば（ステップＳ３１５）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、新たなフレーム鍵計算を行なうフレーム鍵計算状態Ｄ１へ遷移する。

【００９３】（Ｈブランク状態Ｄ４からＶブランク状態Ｄ５への遷移）ＶｓｙｎｃによりＶブランクであることが分かる。Ｖｓｙｎｃを受け取ると（ステップＳ３１６）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、Ｖブランク状態Ｄ５へ遷移する。Ｖブランク状態Ｄ５において、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、終了条件を待つ。

【００９４】（Ｖブランク状態Ｄ５からフレーム鍵計算状態Ｄ１への遷移）ＣＴＬ３信号が発生すれば（ステップＳ３１７）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、新たなフレーム鍵計算を行なうため、フレーム鍵計算状態Ｄ１へ遷移する。

（Ｖブランク状態Ｄ５からアイドル状態Ｄ０への遷移）Ｖブランク期間中に、ＣＴＬ３信号が発生する前に、ＤＥ信号により映像信号に戻った場合（ステップＳ３１９）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、次のフレームの暗号化は行なわない。これはリンクでの認証失敗などにより起こる。

【００９５】（フレーム鍵計算状態Ｄ１から音声暗号化［復号］状態Ｄ６への遷移）Ｖブランク期間中、音声信号の開始信号ＡＤＥがあれば（ステップＳ３０５）、ＨＤＣＰ暗号部２１５＜ＨＤＣＰ復号部３１５＞は、音声信号の暗号化［復号］を始める。音声暗号化［復号］状態Ｄ６において、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、音声信号を暗号化［復号］する。

【００９６】（音声暗号化［復号］状態Ｄ６から映像信号待状態Ｄ７への遷移）音声信号の終わりがＡＤＥにより通知されると（ステップＳ３０６）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像信号が始まるのを待つ映像信号待状態Ｄ７へ遷移する。図１２において、この信号を「！ＡＤＥ」と表現している。

【００９７】（映像信号待状態Ｄ７から映像暗号化［復号］状態Ｄ２への遷移）ＴＭＤＳリンクのＤＥ信号は暗号化［復号］すべき映像信号の先頭を与える。ＤＥ信号を受け取ると（ステップＳ３０７）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像暗号化［復号］状態Ｄ２へ遷移する。（Ｈブランク状態Ｄ４から音声暗号化［復号］状態Ｄ８への遷移）ＡＤＥ信号を受け取り（ステップＳ３１１）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、次のＨブランキング期間の音声信号の暗号化［復号］を始めるために、音声暗号化［復号］状態Ｄ８へ遷移する。

【００９８】音声暗号化［復号］状態Ｄ８において、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、音声

信号を暗号化［復号］する。（音声暗号化［復号］状態Ｄ８から映像信号待状態Ｄ９への遷移）音声信号の終わりがＡＤＥにより通知されると（ステップＳ３１２）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像信号待状態Ｄ９へ遷移する。

【００９９】映像信号待状態Ｄ９において、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像信号が始まるのを待つ。（映像信号待状態Ｄ９から映像暗号化［復号］状態Ｄ２への遷移）ＴＭＤＳリンクのＤＥ信号は暗号化［復号］すべき映像信号の先頭を与える。ＤＥ信号を受け取ると（ステップＳ３１３）、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］は、映像暗号化［復号］状態Ｄ２へ遷移する。

【０１００】３．まとめ

以上説明した本実施の形態によると、映像信号及び音声信号を時分割多重して暗号伝送する暗号伝送システムは、送信側において、音声信号を時間軸圧縮し、該時間軸圧縮した音声信号を、映像信号のブランキング期間に多重して暗号伝送する。

【０１０１】また、前記暗号伝送システムは、前記送信側において、受信側の認証の後、及び垂直同期信号の後にフレーム用の鍵を計算し、計算したフレーム用の鍵を用いて時間圧縮した音声信号を暗号化し、その後映像信号を暗号化し、さらに、鍵の更新を行って、水平同期信号の後に前記更新された鍵を用いて次の時間圧縮した音声信号を暗号化し、その後次の映像信号を暗号化する。

【０１０２】また、前記暗号伝送システムは、前記受信側において、送信側との認証の後、及び垂直同期信号の後にフレーム用の鍵を計算し、計算したフレーム用の鍵を用いて暗号化された音声信号を復号し、その後暗号化された映像信号を復号し、さらに、鍵の更新を行って、水平同期信号の後に前記更新された鍵を用いて次の暗号化された音声信号を復号し、その後次の暗号化された映像信号を復号する。

【０１０３】また、前記暗号伝送システムは、前記送信側において、音声信号の暗号化送信を音声信号イネーブル信号で受信側に通知し、映像信号の暗号化送信を映像信号イネーブル信号で受信側に通知し、一方、前記受信側では音声信号イネーブル信号がある場合に、音声信号の復号をして、映像信号イネーブル信号がある場合に、映像信号の復号をする。

【０１０４】このように、前記暗号伝送システムにおいては、従来例における映像信号のデータイネーブル信号（DE信号）に加えて、音声信号のデータイネーブル信号（ADE信号）を追加し、これを多重制御信号として用いて制御する。この信号を追加しているので、音声信号の多重がない場合にも受信側で送信側に対応した処理を行うことができる。

【０１０５】また、前記暗号伝送システムは、前記送信側及び受信側のそれぞれにおける映像信号の暗号化及び音声信号の暗号化において、同じ暗号方式を用いる。また、前記暗号伝送システムは、前記暗号方式が内部状態を持つ場合、ある初期状態を設定して音声信号を暗号化し、その後、暗号方式の内部状態をもとの初期状態に戻して、次の映像信号を暗号化する。

【０１０６】ＨＤＣＰで用いているＨＤＣＰ　Ｃｉｐｈｅｒは、内部状態を保持し、これに依存して入力データを暗号化すると同時に内部状態を変更されるタイプの暗号方式である。送信側では、状態Ｄ３時点での暗号方式の内部状態を保存しておき、音声信号を処理（状態Ｄ８）したあと、状態Ｄ９の時点で保存しておいた内部状態に戻して、次の映像信号の暗号化処理（状態Ｄ２）をする。このことにより、受信側で、映像信号しか処理できないＨＤＣＰ対応受信機であっても、映像信号を復号する時点での、送信側と受信側で暗号方式の内部状態が同じになり（つまり、状態Ｄ９から状態Ｄ２の遷移と、状態Ｄ４から状態Ｄ２への遷移）、ＨＤＣＰ受信機は正しく映像信号を処理することができる。

【０１０７】また、前記暗号伝送システムは、前記送信側、及び受信側のそれぞれにおける認証と鍵計算、及び映像信号の暗号化と音声の暗号化において、共通の演算モジュールを用いる。このように、前記暗号伝送システムは、音声信号と映像信号で用いる暗号アルゴリズムを共通にしているので、従来の暗号伝送システムからの追加部分が最小に抑えられる。また、HDCPと同様に認証と鍵共有、暗号化に共通の演算モジュールを用いるているので、実装規模を削減することができる。

【０１０８】また、前記暗号伝送システムは、前記送信側において、前記映像信号及び前記音声信号を、多重制御信号を用いて多重化し、一方、受信側において、送信側から送られた多重制御信号を用いてこれを分離する。また、本実施の形態によると、多重制御信号を送信側から受信側に送るものとしているが、音声信号の処理と映像信号の処理の間に、あらかじめ決められた長さの無信号期間を設け、これを受信側で認識することにより、音声信号と映像信号の切り替えを行うとしてもよい。このようにして、前記暗号伝送システムは、前記多重制御信号を送信側から受信側に送付する代わりに、音声信号と映像信号の間の切り替わりに無信号期間を設け、受信側でこれを認識して多重制御信号を生成する。

【０１０９】以上のように、本実施の形態によれば、 HDCP規格の状態遷移、および実装規模を最小限拡張することにより、従来の映像信号のみならず、そのブランキング期間に時間軸圧縮した音声信号を多重して暗号化伝送することができる。従来のHDCP規格に音声信号の切り替え部を追加して、音声信号のイネーブル信号と切り替え信号で制御する。この制御により、音声信号が多重されない場合については従来のHDCP規格と同じ処理が可能である。なお、切り替え信号の追加が難しい場合は、データ信号上にある特定の長さの無信号区間を設けること

により、受信部で検知して切り替えを行うとしてもよい。

【０１１０】また、従来のHDCP規格と上位互換性を保ちつつ、これを規格上および実装上において最小限に拡張して、映像信号とともに音声信号を暗号化伝送できる。さらに、従来のHDCP規格に準じた受信機においても暗号化映像信号が復号再生できる。また、音声信号の暗号化には映像信号と同じ暗号方式を用いることにより、追加のモジュールも最小となりコンパクトな実装が可能となる。また、各ラインにおける音声信号の暗号化のあと、暗号方式の内部状態を各ラインでの初期状態に戻すことにより、受信機が拡張仕様に対応していない従来のHDCP規格のもの、つまり映像信号の復号しかできない場合であっても、映像信号を正しく復号することができる。

【０１１１】４．その他の実施の形態

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）本実施の形態によると、パーソナルコンピュータにより実現されているが、これには限定されない。デジタル放送受信装置、ＤＶＤ再生装置などにおいて、デジタル音声の付加されたデジタル映像の再生するとしてもよい。

【０１１２】（２）本実施の形態によると、符号化音声情報を、チャネルＣ１２、Ｃ１１及びＣ１０の全てを介して、ビデオ接続部２０１からビデオ接続部３０１へ伝送するとしているが、符号化音声情報の伝送量を少なくし、前記チャネルの内の１個、又は２個のみを介して、伝送するとしてもよい。また、本実施の形態によると、符号化音声情報を、垂直帰線期間及び水平帰線期間において、ビデオ接続部２０１からビデオ接続部３０１へ伝送するとしているが、垂直帰線期間においてのみ、伝送するとしてもよい。また、水平帰線期間においてのみ、伝送するとしてもよい。

【０１１３】（３）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ―ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０１１４】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０１１５】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（４）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１１６】（産業上の利用の可能性）パーソナルコンピュータや情報処理端末などにおいて、映像と音声とを出力する場合において利用することができる。また、ＤＶＤ再生装置やデジタル放送受信装置において、映像と音声とを出力する場合においても利用することができる。

【０１１７】

【発明の効果】上記に説明したように、本発明は、デジタル映像情報を帰線期間を置いて送信する送信装置と、前記デジタル映像情報を受信する受信装置とから構成される伝送システムであって、前記送信装置は、前記帰線期間においてデジタル音声情報を送信し、前記受信装置は、前記帰線期間において前記デジタル音声情報を受信する。

【０１１８】これによって、映像情報と音声情報とを高品質で送受信することができる。また、本発明は、帰線期間を置いてデジタル映像情報を含むフレーム情報を生成し、暗号化して送信する送信装置と、暗号化された前記フレーム情報を受信して復号し、復号されたフレーム情報から前記デジタル映像情報を抽出し、表示する映像表示装置とから構成される暗号伝送システムであって、前記送信装置は、デジタル音声情報を前記帰線期間において前記フレーム情報に多重化し、前記デジタル音声情報が多重化されたフレーム情報を暗号化して送信し、前記映像表示装置は、暗号化された前記フレーム情報を受信し、復号してフレーム情報を生成し、生成した前記フレーム情報内に置かれた前記帰線期間から前記デジタル音声情報を抽出し、音声信号に変換する。

【０１１９】これによって、映像情報と音声情報とを高品質で送受信し、かつ著作物としての保護ができる。

【図面の簡単な説明】

【図１】図１は、パーソナルコンピュータシステム１０の外観を示す外観図である。

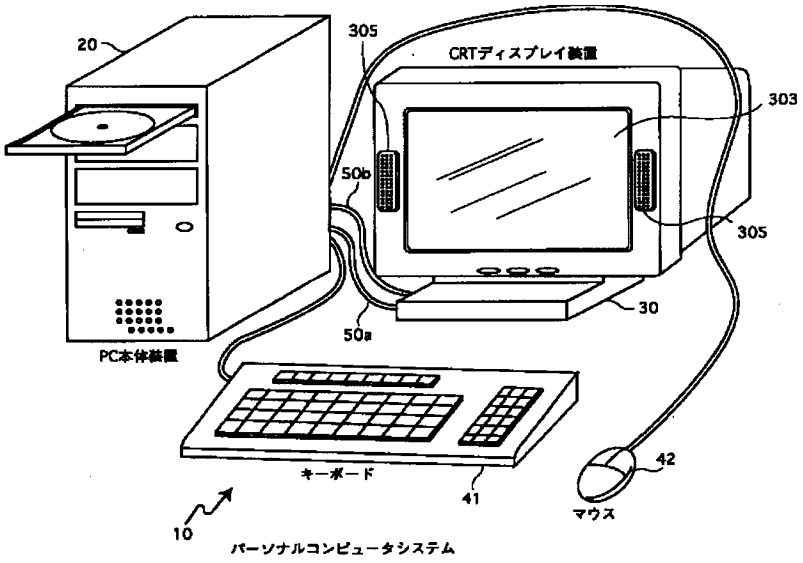
【図２】図２は、パーソナルコンピュータシステム１０の構成を示すブロック図である。

【図３】図３は、ビデオ接続部２０１及びビデオ接続部３０１の構成を示すブロック図である。

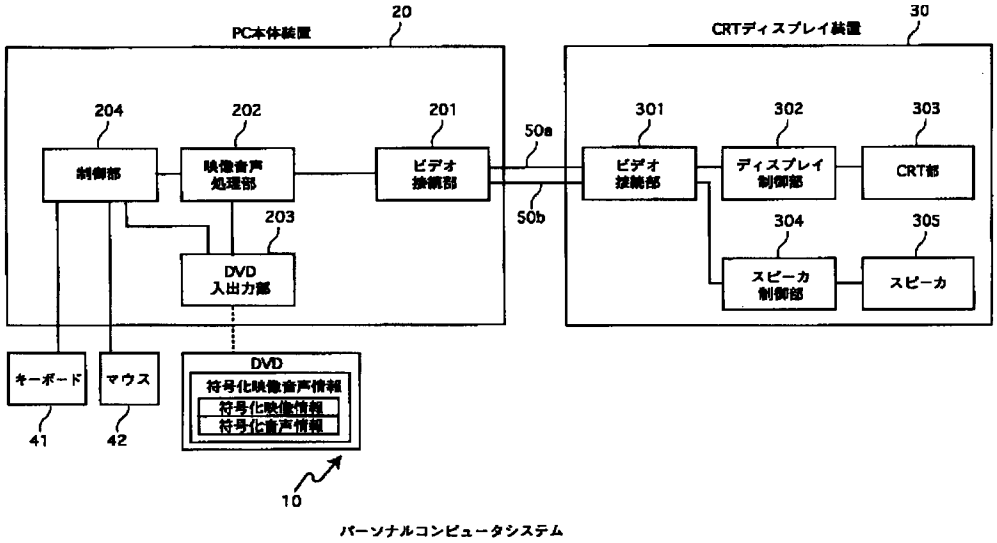
【図４】図４は、垂直帰線期間、水平帰線期間及び１フレーム分の映像情報の関係を示す概念図である。
【図５】図５は、時間の経過に伴う１フレームに相当するデータイネーブル信号ＤＥ、ＡＤＥ、復号映像情報及び符号化音声情報の変化を示す。
【図６】図６は、時間の経過に伴う１ラインに相当するデータイネーブル信号ＤＥ、ＡＤＥ、復号映像情報及び符号化音声情報の変化を示す。
【図７】図７は、ＴＭＤＳ符号化部２１３及びＴＭＤＳ復号部３１１の構成を示すブロック図である。
【図８】図８は、符号化映像音声情報を再生する場合のパーソナルコンピュータシステム１０の概要動作を示すフローチャートである。
【図９】図９は、装置認証の動作を示すフローチャートである。
【図１０】図１０は、フレーム毎の鍵共有の動作を示すフローチャートである。
【図１１】図１１は、１ライン内の音声情報及び映像情報の暗号化、送信及び復号の動作を示すフローチャートである。
【図１２】図１２は、ＨＤＣＰ暗号部２１５［ＨＤＣＰ復号部３１５］による暗号化［復号］の状態遷移を示す遷移チャートである。
【符号の説明】

１０	パーソナルコンピュータシステム
２０	ＰＣ本体装置
３０	ＣＲＴディスプレィ装置
４１	キーボード
４２	マウス
５０ａ	ケーブル
５０ｂ	ケーブル
２０１	ビデオ接続部
２０２	映像音声処理部
２０３	ＤＶＤ入出力部
２０４	制御部
２１１	多重部
２１２	暗号部
２１３	ＴＭＤＳ符号化部
２１４	認証鍵共有部
２１５	ＨＤＣＰ暗号部
３０１	ビデオ接続部
３０２	ディスプレィ制御部
３０３	ＣＲＴ部
３０４	スピーカ制御部
３０５	スピーカ
３１１	ＴＭＤＳ復号部
３１２	暗号部
３１３	分離部
３１４	認証鍵共有部
３１５	ＨＤＣＰ復号部

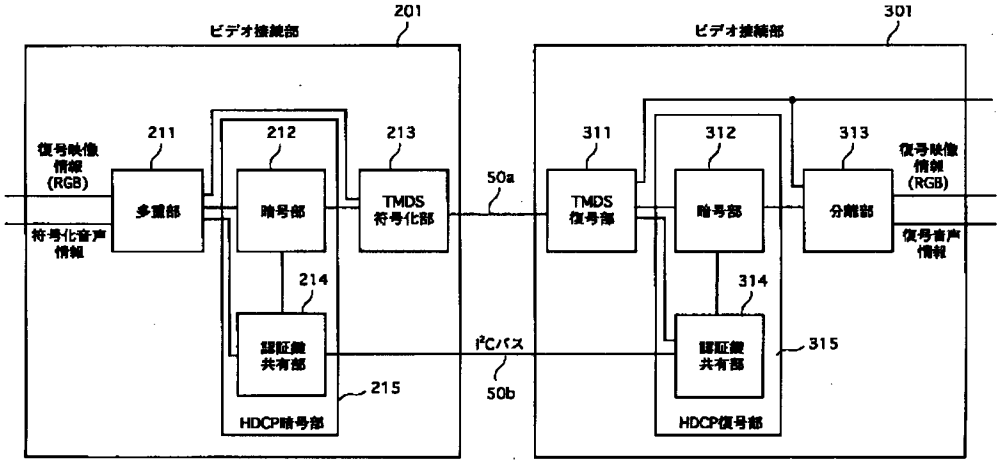
【図１】



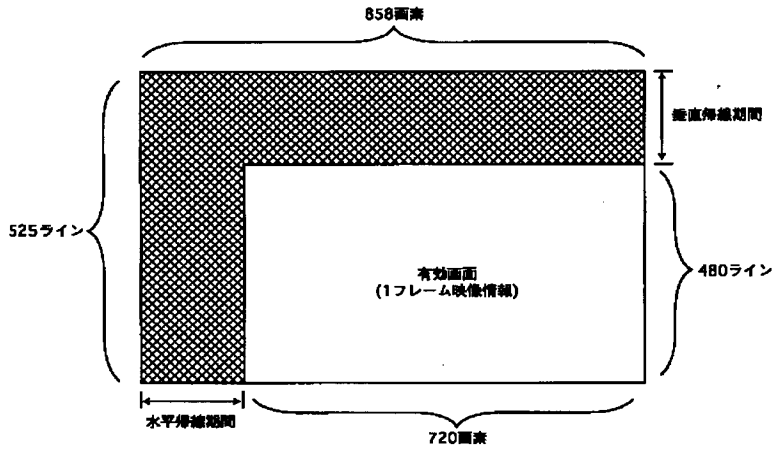
【図２】


PC本体装置
20
CRTディスプレイ装置
30
204
202
201
301
302
303
制御部
映像音声処理部
ビデオ接続部
50a
ビデオ接続部
ディスプレイ制御部
CRT部
50b
203
304
305
DVD入出力部
スピーカ制御部
スピーカ
DVD
符号化映像音声情報
符号化映像情報
符号化音声情報
キーボード
マウス
41
42
10
パーソナルコンピュータシステム

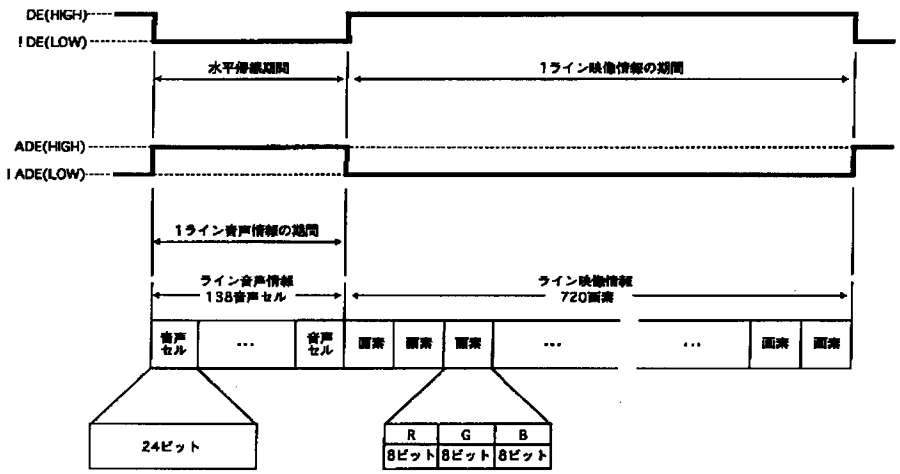
【図３】


ビデオ接続部
201
ビデオ接続部
301
復号映像情報(RGB)
211
212
213
311
312
313
復号映像情報(RGB)
多重部
暗号部
TMDS符号化部
50a
TMDS復号部
暗号部
分離部
符号化音声情報
復号音声情報
214
314
認証鍵共有部
I²Cバス
315
認証鍵共有部
50b
215
HDCP暗号部
HDCP復号部

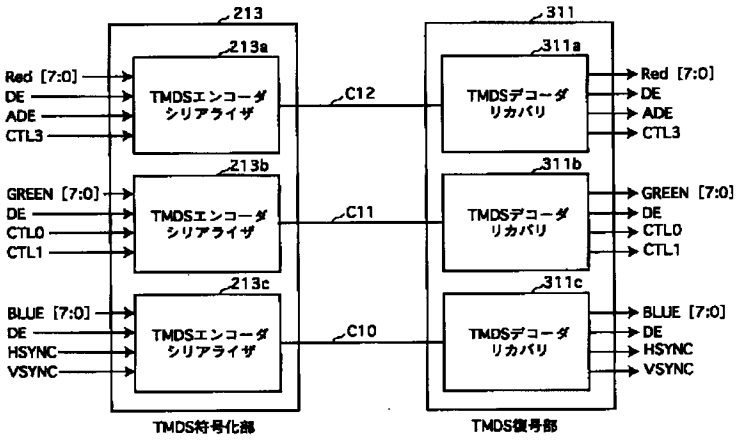
【図４】


858画素
垂直帰線期間
525ライン
有効画面
(1フレーム映像情報)
480ライン
水平帰線期間
720画素

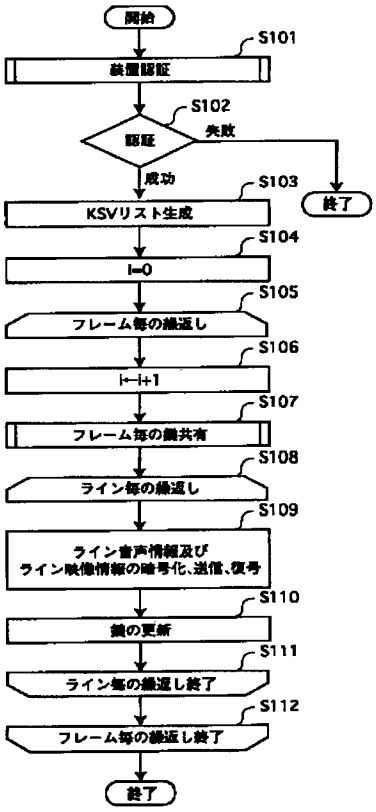
【図６】


DE(HIGH)
!DE(LOW)
水平帰線期間
1ライン映像情報の期間
ADE(HIGH)
!ADE(LOW)
1ライン音声情報の期間
ライン音声情報
138音声セル
ライン映像情報
720画素
音声セル
画素
24ビット
R
G
B
8ビット
8ビット
8ビット

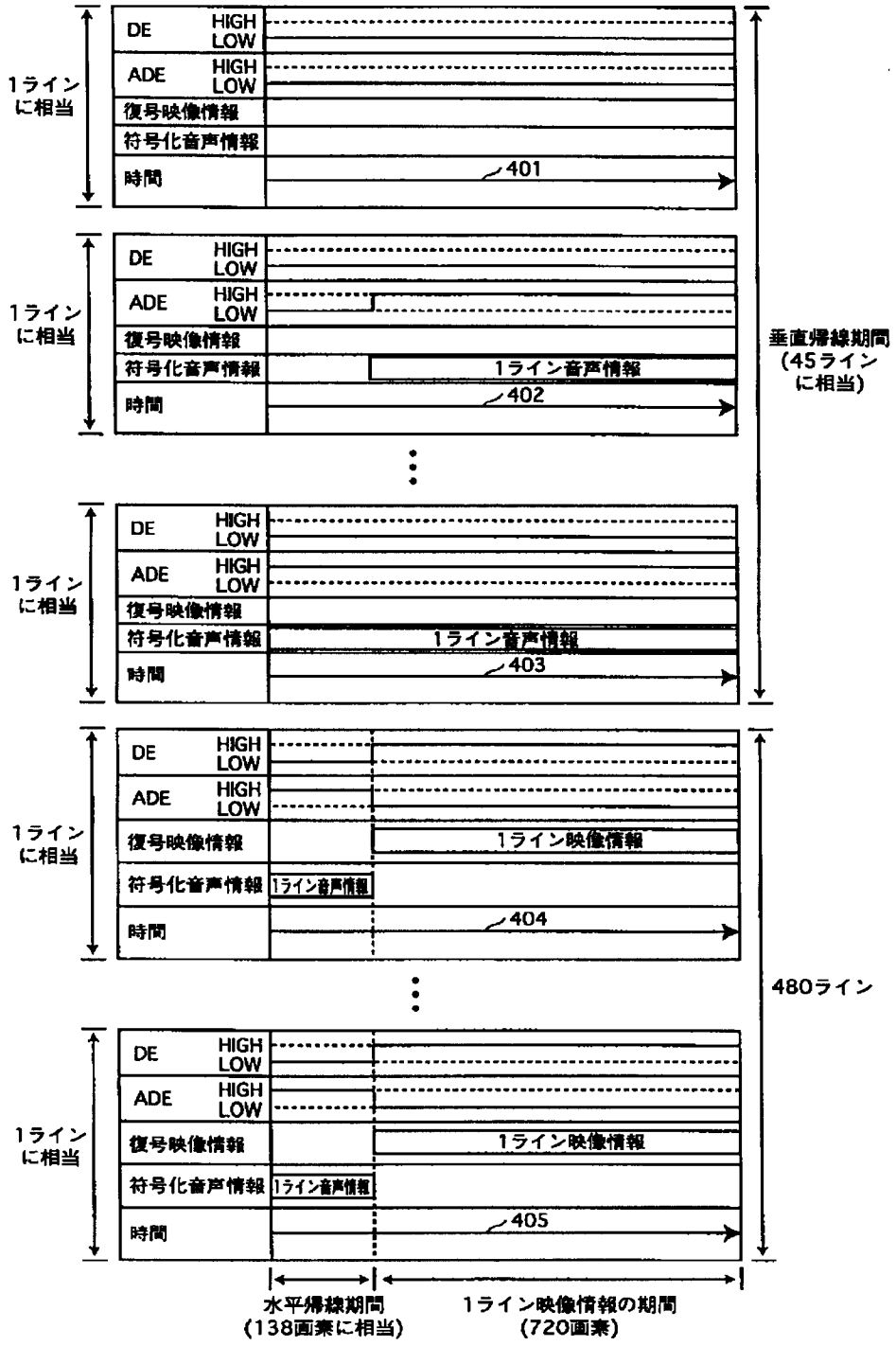
【図７】


213
213a
213b
213c
TMDSエンコーダ
シリアライザ
Red [7:0]
DE
ADE
CTL3
GREEN [7:0]
DE
CTL0
CTL1
BLUE [7:0]
DE
HSYNC
VSYNC
C12
C11
C10
311
311a
311b
311c
TMDSデコーダ
リカバリ
Red [7:0]
DE
ADE
CTL3
GREEN [7:0]
DE
CTL0
CTL1
BLUE [7:0]
DE
HSYNC
VSYNC
TMDS符号化部
TMDS復号部

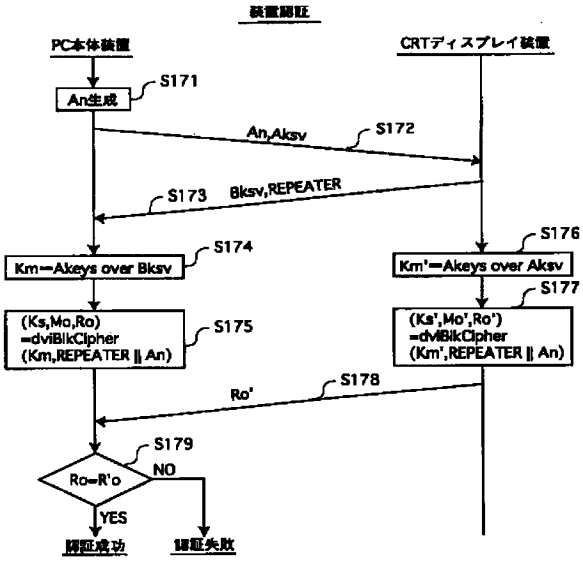
【図８】


開始
S101
装置認証
S102
認証
失敗
成功
終了
S103
KSVリスト生成
S104
i=0
S105
フレーム毎の繰返し
S106
i←i+1
S107
フレーム毎の鍵共有
S108
ライン毎の繰返し
S109
ライン音声情報及び
ライン映像情報の暗号化、送信、復号
S110
鍵の更新
S111
ライン毎の繰返し終了
S112
フレーム毎の繰返し終了
終了

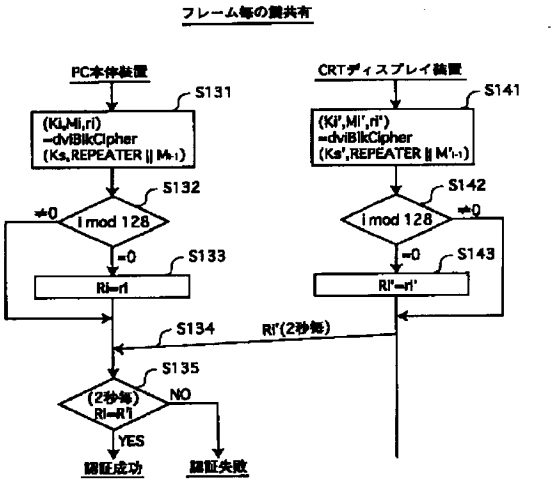
【図５】


1ラインに相当
DE
HIGH
LOW
ADE
復号映像情報
符号化音声情報
時間
401
1ライン音声情報
402
403
1ライン映像情報
404
405
垂直帰線期間
(45ラインに相当)
480ライン
水平帰線期間
(138画素に相当)
1ライン映像情報の期間
(720画素)

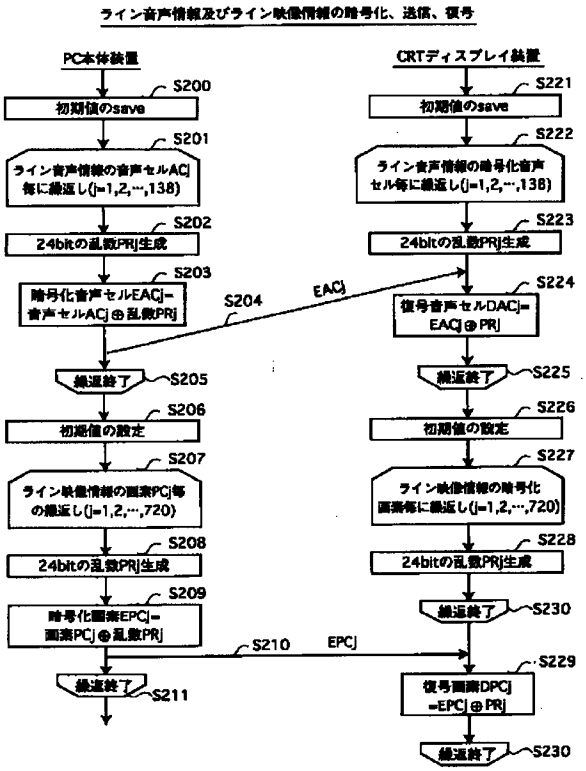
【図９】


装置認証
PC本体装置
CRTディスプレイ装置
An生成
S171
An,Aksv
S172
Bksv,REPEATER
S173
Km=Akeys over Bksv
S174
Km'=Akeys over Aksv
S176
(Ks,Mo,Ro)
=dviBlkCipher
(Km,REPEATER || An)
S175
(Ks',Mo',Ro')
=dviBlkCipher
(Km',REPEATER || An)
S177
Ro'
S178
Ro=R'o
S179
NO
YES
認証成功
認証失敗

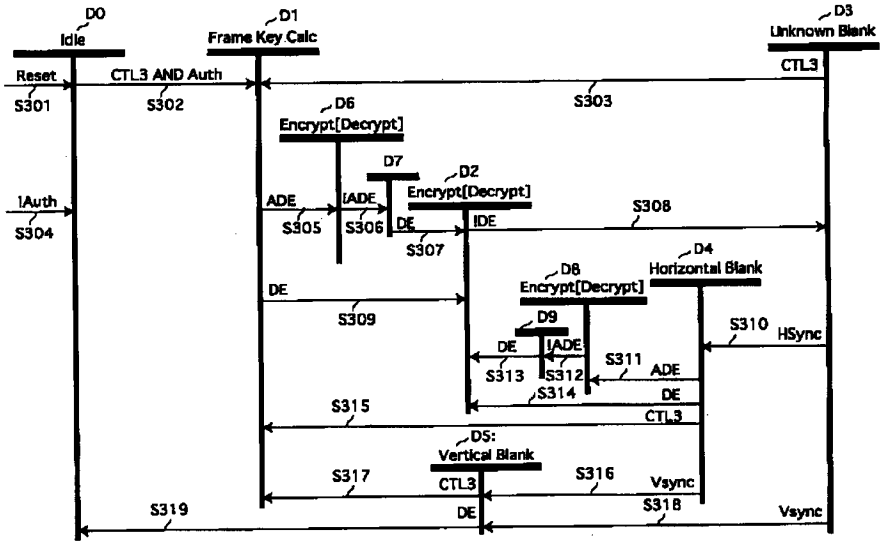
【図１０】


フレーム毎の鍵共有
PC本体装置
CRTディスプレイ装置
(Ki,Mi,ri)
=dviBlkCipher
(Ks,REPEATER || Mi-1)
S131
(Ki',Mi',ri')
=dviBlkCipher
(Ks',REPEATER || M'i-1)
S141
i mod 128
S132
S142
≠0
=0
Ri=ri
S133
Ri'=ri'
S143
S134
Ri'(2秒毎)
(2秒毎)
Ri=Ri'i
S135
NO
YES
認証成功
認証失敗

【図１１】


ライン音声情報及びライン映像情報の暗号化、送信、復号
PC本体装置
CRTディスプレイ装置
初期値のsave
S200
S221
ライン音声情報の音声セルACj
毎に繰返し(j=1,2,…,138)
S201
ライン音声情報の暗号化音声
セル毎に繰返し(j=1,2,…,138)
S222
24bitの乱数PRj生成
S202
S223
暗号化音声セルEACj=
音声セルACj ⊕ 乱数PRj
S203
S204
EACj
復号音声セルDACj=
EACj ⊕ PRj
S224
繰返終了
S205
S225
初期値の設定
S206
S226
ライン映像情報の画素PCj毎
の繰返し(j=1,2,…,720)
S207
ライン映像情報の暗号化
画素毎に繰返し(j=1,2,…,720)
S227
24bitの乱数PRj生成
S208
S228
暗号化画素EPCj=
画素PCj ⊕ 乱数PRj
S209
S230
S210
EPCj
繰返終了
S211
復号画素DPCj
=EPCj ⊕ PRj
S229
S230

【図１２】



フロントページの続き

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｎ　7/088			

(72)発明者　西尾　歳朗
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　鈴木　秀和
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5C063 AB03 AC01 AC05 CA20 DA07 DA13 DB01
5J104 BA04 BA06 FA06